PCT/JP2004/014667

29. 9. 2004

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年１１月 ７日

出願番号
Application Number: 特願２００３－３７８５７４

[ST. 10/C]: [ＪＰ２００３－３７８５７４]

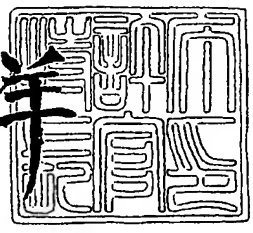
出願人
Applicant(s): 松下電器産業株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００４年１１月 ５日

特許庁長官
Commissioner,
Japan Patent Office

小 川 洋



出証番号 出証特２００４－３０９９９４８

【書類名】　特許願
【整理番号】　2048150034
【あて先】　特許庁長官殿
【国際特許分類】　G06F 12/14
H04N 5/7617
H04N 5/915
H04N 7/16
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　東　吾紀男
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　岡本　隆一
【特許出願人】
【識別番号】　000005821
【氏名又は名称】　松下電器産業株式会社
【代理人】
【識別番号】　100109210
【弁理士】
【氏名又は名称】　新居　広守
【手数料の表示】
【予納台帳番号】　049515
【納付金額】　21,000円
【提出物件の目録】
【物件名】　特許請求の範囲　1
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　0213583

【書類名】特許請求の範囲
【請求項１】
コンテンツを配信するコンテンツ配信サーバと、前記コンテンツの利用をセキュアに制御する端末装置と、から構成されるコンテンツ利用制御システムであって、
前記コンテンツ配信サーバは、
時刻情報を前記コンテンツに付加する時刻情報付加部と、
前記時刻情報を用いて、前記コンテンツの特定部分の利用を制御するための利用制御情報を、前記コンテンツとは別データとして生成する利用制御情報生成部と、
前記時刻情報を前記コンテンツにセキュアにバインドする時刻情報バインド部と、
を備え、
前記端末装置は、
前記コンテンツを利用するコンテンツ利用部と、
前記コンテンツに付加されたセキュアな前記時刻情報と前記利用制御情報とを用いて、前記コンテンツ利用部での前記コンテンツの利用をセキュアに制御するコンテンツ利用制御部と、
を備えることを特徴とするコンテンツ利用制御システム。
【請求項２】
前記利用制御情報は、前記コンテンツの特殊再生を禁止する
ことを特徴とする請求項１記載のコンテンツ利用制御システム。
【請求項３】
前記利用制御情報は、前記コンテンツのプレビューを許可する
ことを特徴とする請求項１記載のコンテンツ利用制御システム。
【請求項４】
前記利用制御情報は、前記コンテンツの利用許可を与えるライセンスに設定される
ことを特徴とする請求項１記載のコンテンツ利用制御システム。
【請求項５】
前記利用制御情報は、デジタル放送のＥＣＭ（Ｅｎｔｉｔｌｅｍｅｎｔ　Ｃｏｎｔｒｏｌ　Ｍｅｓｓａｇｅ）に設定される
ことを特徴とする請求項１記載のコンテンツ利用制御システム。
【請求項６】
前記利用制御情報は、許可された利用または操作の種別を含む
ことを特徴とする請求項１記載のコンテンツ利用制御システム。
【請求項７】
前記利用制御情報は、特定の利用または操作が許可されるまでの回数または時間に関する制限を含む
ことを特徴とする請求項１記載のコンテンツ利用制御システム。
【請求項８】
前記利用制御情報は、許可された利用または操作の回数または時間に関する制限を含む
ことを特徴とする請求項１記載のコンテンツ利用制御システム。
【請求項９】
前記時刻情報は、ＭＰＥＧ－２　ＳｙｓｔｅｍｓのＰＥＳパケットに設定されたＰＴＳ（Ｐｒｅｓｅｎｔａｔｉｏｎ　Ｔｉｍｅ　Ｓｔａｍｐ）である
ことを特徴とする請求項１記載のコンテンツ利用制御システム。
【請求項１０】
前記コンテンツ利用制御部は、前記利用制御情報を未取得である場合、前記コンテンツの通常利用のみを許可する
ことを特徴とする請求項１記載のコンテンツ利用制御システム。
【請求項１１】
前記コンテンツ利用制御部は、前記利用制御情報を未取得である場合、前記コンテンツの特殊再生を禁止する

ことを特徴とする請求項２記載のコンテンツ利用制御システム。
【請求項１２】
　前記コンテンツ利用制御部は、前記利用制御情報を未取得である場合、前記コンテンツのプレビューを禁止する
ことを特徴とする請求項３記載のコンテンツ利用制御システム。
【請求項１３】
　前記端末装置は、少なくとも前記コンテンツの視聴箇所を含む視聴履歴を記録する視聴履歴記録部をさらに備え、
　前記コンテンツ利用制御部は、前記利用制御情報に加え、さらに前記視聴履歴を用いて前記コンテンツ利用部での前記コンテンツの利用をセキュアに制御する
ことを特徴とする請求項１記載のコンテンツ利用制御システム。
【請求項１４】
　前記コンテンツのリアルタイム視聴時と蓄積視聴時とで、前記コンテンツ利用制御部によって利用制御される前記コンテンツの箇所が異なる
ことを特徴とする請求項１記載のコンテンツ利用制御システム。

【書類名】明細書
【発明の名称】コンテンツ利用制御システム
【技術分野】
【０００１】
本発明は、通信や放送を用いて、サーバ装置から映像、音楽などのデジタルコンテンツを配信し、ユーザが端末装置でデジタルコンテンツを利用するシステムに関し、特に、端末装置におけるデジタルコンテンツの特定部分について、タイムスキップや早送りなどの特殊再生を、事業者の意図に従って確実に制御することが可能なシステムに関する。
【背景技術】
【０００２】
近年、音楽、映像、ゲームなどのデジタルコンテンツ（以下、コンテンツと記述）を、インターネットなどの通信や、デジタル放送、ＣＡＴＶ（Ｃａｂｌｅ　Ｔｅｌｅｖｉｓｉｏｎ）などを通じて、サーバ装置から端末装置に配信し、端末装置においてコンテンツを利用することが可能なコンテンツ配信サービスが実用化段階に入っている。このコンテンツ配信サービスに用いられる一般的なシステムでは、コンテンツの著作権を保護し、悪意あるユーザなどによるコンテンツの不正利用を防止するため、著作権保護技術が用いられる。著作権保護技術とは、具体的には、暗号技術や認証技術などを用いて、ユーザがコンテンツを再生したり、記録メディアにコピーしたりといったようなコンテンツの利用を、セキュアに制御する技術である。著作権保護技術を用いることにより、コンテンツプロバイダやサービスプロバイダなどの事業者が、ユーザの端末装置におけるコンテンツ利用をセキュアに制御することが可能となる。
【０００３】
ところで、近年、ＨＤＤ（Ｈａｒｄ　Ｄｉｓｋ　Ｄｒｉｖｅ）などの大容量蓄積手段を有する端末装置において、配信されたコンテンツを一旦端末装置に蓄積し、ユーザが好きなときに好きなコンテンツを視聴するという、ユーザ利便性の高い利用形態が検討されている。日本におけるデジタル放送の規格化団体であるＡＲＩＢ（Ａｓｓｏｃｉａｔｉｏｎ　ｏｆ　Ｒａｄｉｏ　Ｉｎｄｕｓｔｒｉｅｓ　ａｎｄ　Ｂｕｓｉｎｅｓｓｅｓ）においても、大容量蓄積機能を活用するデジタル放送方式として、サーバ型放送方式が規格化されている。サーバ型放送方式に関しては、ＡＲＩＢ　ＳＴＤ－Ｂ２５　４．１版が詳しい。
【０００４】
しかしながら、このような蓄積機能を有する端末装置においては、コマーシャル（ＣＭ）を含んだコンテンツを一旦端末装置に蓄積し、タイムシフトによる視聴時にＣＭ部分をスキップしたり、早送りしたりすることにより、ユーザがＣＭを視聴しないという事態が発生しうる。その結果として、事業者にとってＣＭ効果が小さくなり、ＣＭ料金が低下するなどといったデメリットが発生する可能性がある。このような課題を解決する技術として、例えば、特許文献１には、サーバ装置でコンテンツのＣＭ部分の前後にＣＭスキップ禁止信号、または、ＣＭスキップ禁止解除信号を埋め込んでおくことにより、端末装置においてＣＭスキップの制御を行うシステムが、コンテンツ利用制御システムの一例として記載されている。
【０００５】
このように、従来のコンテンツ利用制御システムでは、コンテンツのＣＭ部分など、コンテンツ提供者側で特殊再生を禁止したい部分に、その旨を示す制御情報を埋め込んでおくことによって、事業者の意図に反したユーザのコンテンツ利用を防止することができるようになっている。
【特許文献１】特開２００２－２９０８７８号公報
【発明の開示】
【発明が解決しようとする課題】
【０００６】
しかしながら、従来のコンテンツ利用制御システムでは、ＣＭ部分の特殊再生を防止するため、コンテンツにＣＭ視聴を制御するための制御情報を埋め込む必要がある。通常、

コンテンツをデジタル符号化するエンコーダには、コンテンツのＣＭ部分を識別する機能はもちろんのこと、ＣＭ視聴制御のための情報を挿入する機能ですら有していないのが一般的である。よって、ＣＭ視聴を制御可能なコンテンツを生成するためには、専用のエンコーダが必要であり、その結果、事業者のコスト負担が大きくなるという課題があった。

【０００７】

本発明は、こうした従来の問題点を解決するものであり、コンテンツに制御情報を追加することなく、端末装置でのコンテンツのＣＭ部分などのコンテンツの特定部分の利用制御をセキュアに実現することにより、低廉なコストで事業者の意図に反するユーザのコンテンツ利用を防止することが可能なコンテンツ利用制御システムを提供することを目的としている。

【課題を解決するための手段】

【０００８】

上記目的を達成するために、本発明に関わるコンテンツ利用制御システムは、コンテンツを配信するコンテンツ配信サーバと、前記コンテンツの利用をセキュアに制御する端末装置とから構成されるコンテンツ利用制御システムであって、前記コンテンツ配信サーバは、時刻情報を前記コンテンツに付加する時刻情報付加部と、前記時刻情報を用いて、前記コンテンツの特定部分の利用を制御するための利用制御情報を、前記コンテンツとは別データとして生成する利用制御情報生成部と、前記時刻情報を前記コンテンツにセキュアにバインドする時刻情報バインド部とを備え、前記端末装置は、前記コンテンツを利用するコンテンツ利用部と、前記コンテンツに付加されたセキュアな前記時刻情報と、前記利用制御情報とを用いて、前記コンテンツ利用部での前記コンテンツの利用をセキュアに制御するコンテンツ利用制御部とを備えることを特徴とする。

【０００９】

本構成によって、コンテンツに利用制御のための特別な情報を挿入することなく、コンテンツの特定部分の利用をセキュアに制御することが可能となる。

【発明の効果】

【００１０】

本発明によれば、ＣＭの視聴を制御するための制御情報をコンテンツ本体に埋め込むことなく、コンテンツに既存のセキュアな時刻情報を用いてセキュアにユーザのＣＭ視聴を制御することができるため、一般的なエンコーダで生成したコンテンツを適用することができ、事業者のコスト負担を軽減することが可能となる。

【発明を実施するための最良の形態】

【００１１】

以下、本発明における実施の形態について、図面を用いて詳細に説明する。

図１は、本発明における実施の形態に関わるコンテンツ利用制御システム１の全体の概略構成を示す図である。

このコンテンツ利用制御システム１は、ネットワークなどを通じて配信センター（すなわち、サービスプロバイダ）から配信される暗号化コンテンツを、ユーザが端末装置において利用する際に、セキュアに再生制御を行うシステムであって、コンテンツやコンテンツの利用許諾を与えるライセンスなどを配信する配信センター１０１と、コンテンツを利用する端末装置１０２ａ～１０２ｃと、これらを相互に接続するネットワーク１０３とから構成されている。

【００１２】

配信センター１０１は、ユーザが所有するコンテンツを利用する権利（利用条件）の管理や、コンテンツのライセンスを生成し、端末装置１０２ａ～１０２ｃに配信を行う権利管理サーバ１０１ａと、端末装置１０２ａ～１０２ｃにコンテンツを配信するコンテンツ配信サーバ１０１ｂと、ユーザに対して課金を行うための課金サーバ１０１ｃと、ネットワーク１０３を通じて端末装置１０２ａ～１０２ｃに各種サービスを提供するためのウェブ画面を送信するウェブサーバ１０１ｄとから構成されている。

【００１３】

権利管理サーバ１０１ａは、ユーザが所有するコンテンツの利用条件を管理し、ユーザに暗号化されたコンテンツを復号するためのライセンスを付与するサーバ装置である。具体的には、権利管理サーバ１０１ａは、ユーザ毎、あるいは、端末装置１０２ａ～１０２ｃ毎に、それぞれが所有するコンテンツの利用条件を管理しておき、ユーザからの要求に基づき、インターネットなどのネットワーク１０３を通じて、ライセンスを端末装置１０２ａ～１０２ｃに配信する。また、デジタル放送やブロードバンドインターネットにおいて、プッシュ型の放送形態のコンテンツを配信する場合は、コンテンツとともにライセンスを配信するため、生成したライセンスをコンテンツ配信サーバ１０１ｂに送信する。

【００１４】

なお、ライセンスは、暗号化コンテンツを復号するための暗号鍵と、コンテンツの利用期限や利用回数などの利用条件などから構成される。ライセンスのデータ構造の例については、後で図を用いて詳細に説明する。

また、ライセンスなどのセキュリティを確保すべきデータを、ネットワーク１０３を通じて、配信センター１０１と端末装置１０２ａ～１０２ｃとの間で送受信する場合には、ＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ）やＴＬＳ（Ｔｒａｎｓｐｏｒｔ　Ｌａｙｅｒ　Ｓｅｃｕｒｉｔｙ）などの安全な認証チャネル（Ｓｅｃｕｒｅ　Ａｕｔｈｅｎｔｉｃａｔｅｄ　Ｃｈａｎｎｅｌ、以下、ＳＡＣと記述）を確立し、データの送受信を行う。

【００１５】

コンテンツ配信サーバ１０１ｂは、ネットワーク１０３を通じて端末装置１０２ａ～１０２ｃにコンテンツを配信するためのサーバ装置であり、専用ハードウェアやワークステーションなどにより実現される。具体的には、コンテンツ配信サーバ１０１ｂは、ＭＰＥＧ－２やＭＰＥＧ－４などの圧縮方式によりデジタル圧縮され、必要に応じて、ＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）やＴｒｉｐｌｅ　ＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）などの共通鍵暗号アルゴリズムなどにより暗号化した上で、暗号化コンテンツをストリーミング配信、あるいは、ダウンロード配信する。

【００１６】

特に、ＢＳ（Ｂｒｏａｄｃａｓｔｉｎｇ　Ｓａｔｅｌｌｉｔｅ）デジタル放送、ＣＳ（Ｃｏｍｍｕｎｉｃａｔｉｏｎ　Ｓａｔｅｌｌｉｔｅ）デジタル放送、地上波デジタル放送におけるサーバ型放送方式では、ＭＰＥＧ－２やＭＰＥＧ－４のコンテンツ（Ｅｌｅｍｅｎｔａｒｙ　Ｓｔｒｅａｍ、以下、ＥＳと記述）を、ＰＥＳ（Ｐａｃｋｅｔｉｚｅｄ　Ｅｌｅｍｅｎｔａｒｙ　Ｓｔｒｅａｍ）／ＴＳ（Ｔｒａｎｓｐｏｒｔ　Ｓｔｒｅａｍ）により多重化された、リアルタイム視聴と蓄積視聴の共用が可能なストリーム型コンテンツを配信する方式が規格化されており、サーバ型放送方式タイプＩと称される。

【００１７】

ここで、図２を用いて、サーバ型放送方式タイプＩをベースとしたコンテンツ配信における暗号鍵スキームについて簡単に説明する。

図２において、コンテンツ・暗号鍵を配信する送信側と、コンテンツ・暗号鍵を受信する受信側に分けて説明する。まず、送信側では、コンテンツはスクランブル鍵Ｋｓ２０１と呼ばれる暗号鍵によって暗号化（２０２）、すなわち、スクランブルされ、受信側に送信される。コンテンツのスクランブルについては、ＭＰＥＧ－２　ＴＳのパケット単位で、ＴＳパケットのペイロード部をスクランブルする。また、スクランブル鍵Ｋｓ２０１は、不正受信に対するセキュリティ向上のため、数秒おきに変更される時変鍵である。

【００１８】

また、コンテンツをスクランブルするスクランブル鍵Ｋｓ２０１は、ワーク鍵Ｋｗ２０３を用いて暗号化（２０４）され、受信側に送信される。ワーク鍵Ｋｗ２０３は、従来の一般的な限定受信方式で用いられている放送事業体毎の契約単位、グループ単位に割り当てられる暗号鍵であり、ワーク鍵Ｋｗ２０３自体のセキュリティを確保するため、数ヶ月～数年の期間で更新されるのが一般的である。少なくともスクランブル鍵Ｋｓ２０１を含

み、コンテンツに関連する情報を送信するためのデータ構造は、ＥＣＭ（Ｅｎｔｉｔｌｅｍｅｎｔ　Ｃｏｎｔｒｏｌ　Ｍｅｓｓａｇｅ）と呼ばれ、ＭＰＥＧ－２　Ｓｙｓｔｅｍｓのプライベートセクションとして構成される。ワーク鍵Ｋｗ２０３で暗号化されたＥＣＭは、ＥＣＭ－Ｋｗと呼ばれ、放送コンテンツのリアルタイム視聴において利用する。

【００１９】

また、コンテンツをスクランブルするスクランブル鍵Ｋｓ２０１は、コンテンツ鍵Ｋｃ２０５を用いて暗号化（２０４）され、受信側に送信される。コンテンツ鍵Ｋｗ２０５は、コンテンツ単位に割り当てられる暗号鍵であり、ＥＣＭ－Ｋｗと同様、ＭＰＥＧ－２　Ｓｙｓｔｅｍｓのプライベートセクションとして構成される。少なくともスクランブル鍵Ｋｓ２０１を含むＥＣＭを、コンテンツ鍵Ｋｃ２０５で暗号化したものをＥＣＭ－Ｋｃと呼び、放送コンテンツの蓄積視聴において利用する。

【００２０】

さらに、コンテンツ鍵Ｋｃ２０５はワーク鍵Ｋｗ２０３で暗号化され、受信側に送信される。少なくともコンテンツ鍵Ｋｃ２０５を含み、ワーク鍵Ｋｗ２０３で暗号化されたＥＣＭをＫｃ配信用ＥＣＭと呼び、放送コンテンツの蓄積視聴において利用する。Ｋｃ配信用ＥＣＭは、ＥＣＭ－Ｋｗ、および、ＥＣＭ－Ｋｃと同様に、ＭＰＧＥ－２　Ｓｙｓｔｅｍｓのプライベートセクションとして構成されるものである。

【００２１】

なお、ＥＣＭ－Ｋｗ、ＥＣＭ－Ｋｃ、Ｋｃ配信用ＥＣＭのデータ構造の例については、後で図を用いて詳細に説明する。

以上のように生成された暗号化コンテンツ、ＥＣＭ－Ｋｗ、ＥＣＭ－Ｋｃ、および、Ｋｃ配信用ＥＣＭは、ＭＰＥＧ－２　ＴＳパケット化され、必要に応じてＰＳＩ（Ｐｒｏｇｒａｍ　Ｓｐｅｃｉｆｉｃ　Ｉｎｆｏｒｍａｔｉｏｎ）／ＳＩ（Ｓｅｒｖｉｃｅ　Ｉｎｆｏｒｍａｔｉｏｎ）などのデータと多重化（２０７）された後、受信側に送信される。

【００２２】

一方、受信側では、暗号化コンテンツ、ＥＣＭ－Ｋｗ、ＥＣＭ－Ｋｃ、および、Ｋｃ配信用ＥＣＭが多重化されたＭＰＥＧ－２　ＴＳパケットを受信し、これらを分離（２１０）して、暗号化コンテンツ、ＥＣＭ－Ｋｗ、ＥＣＭ－Ｋｃ、Ｋｃ配信用ＥＣＭを取得する。

リアルタイム視聴時には、ＥＣＭ－Ｋｗを取得して、あらかじめ受信側が保持しているワーク鍵Ｋｗ２０３によりＥＣＭ－Ｋｗを復号（２１２）して、スクランブル鍵Ｋｓ２０１を取得する。これにより、暗号化コンテンツを復号（２１３）して、コンテンツを利用することが可能となる。なお、ＥＣＭ－Ｋｗは、リアルタイム視聴時のみで使用されるため、図示しない蓄積部に記録する必要はない。

【００２３】

一方、蓄積視聴時には、図示しない蓄積部に記録された暗号化コンテンツ、ＥＣＭ－Ｋｃ、Ｋｃ配布用ＥＣＭを読み出す。ワーク鍵Ｋｗ２０３によりＫｃ配布用ＥＣＭを復号（２１４）して、コンテンツ鍵Ｋｃ２０５を取得する。これによりコンテンツ鍵Ｋｃ２０５によりＥＣＭ－Ｋｃを復号（２１２）し、暗号化コンテンツを復号（２１３）して、コンテンツを利用することが可能となる。

【００２４】

なお、ＡＲＩＢ　ＳＴＤ－Ｂ２５　４．１版では、上記説明に加えて、送信側と受信側とで、ワーク鍵Ｋｗ２０３を共有するための方法について記載されているが、本発明における実施の形態では、送信側と受信側との間でＳＡＣを確立し、通信によりワーク鍵Ｋｗ２０３を共有する場合について説明する。もちろん、ＡＲＩＢ　ＳＴＤ－Ｂ２５　４．１版に記載されているように、ＥＭＭ（Ｅｎｔｉｔｌｅｍｅｎｔ　Ｍａｎａｇｅｍｅｎｔ　Ｍｅｓｓａｇｅ）と呼ばれるデータ構造を利用して、放送を用いてワーク鍵Ｋｗ２０３を配信することによって、送信側と受信側とでワーク鍵Ｋｗ２０３を共有するようにしても良い。この場合、ＥＭＭが盗聴されることを防止するため、マスタ鍵と呼ばれる受信端末毎に固有の鍵で暗号化されて配信される。このマスタ鍵は、送信側と受信側で予め共有さ

れる暗号鍵であり、受信側では端末装置１０２のセキュアな場所で管理されるか、セキュリティモジュールと呼ばれる耐タンパ性の高いモジュールにあらかじめ書き込まれて出荷され、セキュリティモジュールを端末装置１０２に挿入して用いられる。

【００２５】

また、ここでは、ワーク鍵Ｋｗ２０３により暗号化されたＫｃ配信用ＥＣＭを蓄積部（図２に図示せず）に蓄積するにあたり、簡単のため、暗号変換を行わずにそのまま蓄積する場合の例を示したが、ワーク鍵Ｋｗ２０３の定期的または不定期の更新に備えるため、受信側があらかじめ保持する暗号鍵、例えば、複数の端末装置１０２であらかじめ共有している暗号鍵（グループ鍵）や端末装置１０２に固有のマスタ鍵を用いて、Ｋｃ配信用ＥＣＭの暗号変換を行うようにしても良い。

【００２６】

以上、図２を用いて、サーバ型放送方式タイプＩをベースとした暗号鍵スキームについて説明した。以降、本発明における実施の形態では、図２で説明した暗号鍵スキームに基づくコンテンツ利用制御システムについての説明を行う。

また、コンテンツ配信サーバ１０１ｂは、端末装置１０２ａ～１０２ｃでのコンテンツの再生制御を行うため、コンテンツのＣＭ部分やプレビュー部分など、コンテンツにあらかじめ設定された属性情報に基づき、コンテンツの特定箇所の再生制御を行うための再生制御情報を生成して、ＥＣＭとともに端末装置１０２ａ～１０２ｃに配信する。

【００２７】

課金サーバ１０１ｃは、インターネットなどを通じて、コンテンツの利用条件などを購入する際に、オンラインでの課金を行うためのサーバ装置である。具体的には、課金サーバ１０１ｃは、クレジットカードを用いて課金、決済を行ったり、あらかじめ課金サーバ１０１ｃにユーザの銀行口座番号を登録しておき、ネットワーク１０３を経由して端末装置１０２ａ～１０２ｃからアップロードされた購入の履歴などに基づき、課金、決済を行ったりする。

【００２８】

ウェブサーバ１０１ｄは、ユーザが端末装置１０２ａ～１０２ｃから各種サービスにアクセスするためのコンテンツ購入画面などを提供する。具体的には、ウェブサーバ１０１ｄは、インターネットを通じて、ＨＴＴＰなどのプロトコルにより、ＨＴＭＬ（ＨｙｐｅｒＴｅｘｔ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ）やＸＭＬ（Ｅｘｔｅｎｓｉｂｌｅ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ）などのスクリプト言語で記述されたウェブページを提供したり、デジタル放送において、ＢＭＬ（Ｂｒｏａｄｃａｓｔｉｎｇ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ）で記述されたページを提供したりする。

【００２９】

ＬＡＮ１０１ｎは、配信センター１０１において、権利管理サーバ１０１ａと、コンテンツ配信サーバ１０１ｂと、ウェブサーバ１０１ｄと、課金サーバ１０１ｃとを相互に接続するためのネットワークである。例えば、ＩＥＥＥ８０２．３などの有線ネットワークや、ＩＥＥＥ８０２．１１ｂなどの無線ネットワークを用いて実現することができる。

ネットワーク１０３は、配信センター１０１と端末装置１０２ａ～１０２ｃとを相互に接続するネットワークである。例えば、ネットワーク１０３は、インターネットなどの通信ネットワークや、デジタル放送、あるいは、これらが複合したネットワークである。

【００３０】

端末装置１０２ａ～１０２ｃは、ネットワーク１０３と接続する機能を有し、ユーザがコンテンツをモニター画面などで利用したり、記録メディアにコンテンツを書き出したりするための端末装置である。具体的には、端末装置１０２ａ～１０２ｃは、デジタル放送を受信するためのＳＴＢ（Ｓｅｔ　Ｔｏｐ　Ｂｏｘ）、デジタルＴＶ、ＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｃ）レコーダ、ＨＤＤレコーダ、ＰＣ（Ｐｅｒｓｏｎａｌ　Ｃｏｍｐｕｔｅｒ）などのコンテンツ表示装置、レコーダ、あるいは、これらの複合機器である。

【００３１】

このようなコンテンツ利用制御システム１において、デジタル放送やブロードバンドインターネットなどのネットワーク１０３を通じてコンテンツやライセンスが配信され、端末装置１０２ａ～１０２ｃにおいてライセンス、および、再生制御情報に基づきコンテンツを視聴する処理を、図３～図３２の図面を用いて詳細に説明する。但し、以下では、端末装置１０２ａ～１０２ｃについては、端末装置１０２ａをその代表とし、端末装置１０２として説明する。

【００３２】

図３は、図１に示される配信センター１０１における権利管理サーバ１０１ａの詳細な構成を示す機能ブロック図である。

権利管理サーバ１０１ａは、大きく分けて、ＨＤＤなどに格納されたデータファイルなどによって実現されるデータベース部３００と、システムＬＳＩなどのハードウェアあるいはＣＰＵ、ＲＡＭ、ＲＯＭなどを利用して実行されるプログラムなどによって実現されるライセンス処理部３１０とから構成されている。

【００３３】

データベース部３００は、鍵情報ＤＢ３０１、ユーザ情報ＤＢ３０２、利用条件ＤＢ３０３、コンテンツ情報ＤＢ３０４とから構成されている。

鍵情報ＤＢ３０１は、ユーザが事業者（サービスプロバイダ）とサービスを契約することによって与えられるワーク鍵Ｋｗ２０３、および、コンテンツ毎に割り当てられる蓄積視聴時のためのコンテンツ鍵Ｋｃ２０５を管理するデータベースであり、コンテンツ配信サーバ１０１ｂがＥＣＭ－Ｋｗ、ＥＣＭ－Ｋｃ、Ｋｃ配信用ＥＣＭを生成する際にワーク鍵Ｋｗ２０３、コンテンツ鍵Ｋｃ２０５を提供したり、端末装置１０２からワーク鍵Ｋｗ２０３を含むライセンスをリクエストされた際に、ユーザの契約（契約ＩＤ）に対応するワーク鍵Ｋｗ２０３を検索したりする場合に用いられる。

【００３４】

具体的には、鍵情報ＤＢ３０１は、図４に示すように、契約ＩＤ４０１に対応するワーク鍵ＩＤ４０２とワーク鍵Ｋｗ２０３の組を管理するワーク鍵管理テーブル４００を管理する。

例えば、図４では、契約ＩＤ４０１が「ＣＯＮＴＲＡＣＴ－ＩＤ－００００１」に対応するワーク鍵ＩＤ４０２は「Ｋｗ－ＩＤ－００００１」であり、ワーク鍵Ｋｗ２０３が「０ｘ２３４０６８５３４５３１０９１１」であることを示している。ここで、契約ＩＤ４０１とは、事業者が提供するサービスに対する一種の契約形態を示し、例えば、スポーツに関するコンテンツを視聴できる「スポーツコンテンツパック」、映画コンテンツを視聴できる「映画コンテンツパック」などがあげられる。但し、契約ＩＤ毎にワーク鍵Ｋｗ２０３を割り当てるのではなく、サービスプロバイダ毎にワーク鍵Ｋｗ２０３を割り当て、契約ＩＤ４０１の識別をライセンス中に設定される利用条件で判別したり、ＥＣＭの項目として契約ＩＤを含めるようにしたりすることも可能である。また、ワーク鍵ＩＤ４０２は、ＥＣＭを暗号化しているワーク鍵Ｋｗ２０３を特定するために用いられる情報である。

【００３５】

また、鍵情報ＤＢ３０１は、図５に示すように、コンテンツ利用制御システム１においてコンテンツを一意に識別するコンテンツＩＤ５０１と、コンテンツＩＤ５０１に対応するコンテンツ鍵Ｋｃ２０５とからなるコンテンツ鍵管理テーブル５００とを管理する。

例えば、コンテンツＩＤ５０１が「ＣＯＮＴＥＮＴ－ＩＤ－００００１」の暗号化コンテンツを復号するためのコンテンツ鍵Ｋｃ２０５が「０ｘ１２３４５６７８９０ａｂｃｄｅｆ」であることを示している。

【００３６】

ユーザ情報ＤＢ３０２は、ユーザに関する情報を管理するためのユーザ情報管理テーブルを有するデータベースであって、権利管理サーバ１０１ａにアクセスする端末装置１０２と、利用条件ＤＢ３０３で管理される利用条件を所有するユーザとを関連付けるために用いられる。

具体的には、ユーザ情報ＤＢ３０２は、図６に示すユーザ情報管理テーブル６００を有し、コンテンツ利用制御システム１内でユーザを一意に特定するためのユーザＩＤ６０１と、コンテンツ利用制御システム１内で端末装置１０２を一意に特定するための端末ＩＤ６０２とを管理している。

【００３７】

例えば、図６において、ユーザＩＤ６０１が「ＵＳＥＲ－ＩＤ－００００１」であるユーザは、端末ＩＤ６０２が「ＴＥＲＭＩＮＡＬ－ＩＤ－００００１」である端末装置１０２を所有していることを示している。また、ユーザＩＤ６０１が「ＵＳＥＲ－ＩＤ－００００２」であるユーザは、端末ＩＤ６０２が「ＴＥＲＭＩＮＡＬ－ＩＤ－１２３４５」、「ＴＥＲＭＩＮＡＬ－ＩＤ－５４３２１」という２つの端末装置１０２を有しており、両方の端末装置１０２から権利管理サーバ１０１ａにアクセス可能であることを示している。

【００３８】

なお、ユーザ情報ＤＢ３０２へのデータ登録は、ユーザによって、サービスプロバイダが提供するサービスを受けるために会員登録をする際に行なわれる。この会員登録処理は、ユーザがネットワーク１０３を通じてウェブサーバ１０１ｄが提供する会員登録画面により、配信センター１０１と端末装置１０２とがオンラインで行っても良いし、会員登録用の葉書を用いるなど、オフラインで行っても良い。会員登録処理では、まずサービスプロバイダがユーザに対してユーザＩＤ６０１を割り当てる。その後、ユーザが所有する端末装置１０２の端末ＩＤ６０２が、オンラインまたはオフラインによりサービスプロバイダに通知されるので、ユーザＩＤ６０１と端末ＩＤ６０２とが関連付けられて、ユーザ情報ＤＢ３０２のユーザ情報管理テーブル６００に登録される。以上のような会員登録処理を行った結果、ユーザ情報ＤＢ３０２が構築される。

【００３９】

利用条件ＤＢ３０３は、ユーザ毎の事業者との契約に対する利用条件を管理するデータベースであって、端末装置１０２からのライセンス取得要求に対して、ユーザが所有する利用条件を満たすか否かを判定し、利用条件を満たす場合にライセンスを生成するために用いられる。

具体的には、利用条件ＤＢ３０３は、図７に示すように、コンテンツ利用制御システム１においてユーザを一意に識別し、利用条件の所有者を示すユーザＩＤ７０１と、ユーザＩＤ７０１に示されるユーザが所有する利用条件を識別するための利用条件ＩＤ７０２と、コンテンツ利用制御システム１においてユーザの契約形態を一意に識別する契約ＩＤ７０３と、契約ＩＤ７０３で示される契約の開始日時、終了日時を示す有効期間７０４と、契約ＩＤ７０３で示される契約形態に対応するライセンスの発行の残り回数を示す発行可能残回数７０５とからなる利用条件管理テーブル７００を有する。

【００４０】

例えば、ユーザＩＤ７０１が「ＵＳＥＲ－ＩＤ－００００１」であるユーザは、利用条件ＩＤ７０２が「ＵＲＵｓ－ＩＤ－００００１」なる利用条件を保持している。利用条件「ＵＲＵｓ－ＩＤ－００００１」は、ユーザが事業者と結んだ契約が、契約ＩＤ７０３に示される「ＣＯＮＴＲＡＣＴ－ＩＤ－００００１」なる契約であり、有効期間７０４は「２００２／１２／３１～２００３／１／３０」であり、ライセンスとして発行可能な回数が発行可能残回数７０５に示されている「１」回であることを示している。また、ユーザＩＤ７０１が「ＵＳＥＲ－ＩＤ－００００２」であるユーザは、利用条件ＩＤ７０２が「ＵＲＵｓ－ＩＤ－００００２」と「ＵＲＵｓ－ＩＤ－１００１１」という２つの利用条件を有している。このうち、利用条件「ＵＲＵｓ－ＩＤ－００００２」は、契約ＩＤ７０３が「ＣＯＮＴＲＡＣＴ－ＩＤ－１３４５２」なる契約形態に対する利用条件であり、有効期間７０４が「２００２／１２／１～２００２／１２／３１」、発行可能残回数７０５が「１」であるので、上記有効期間を有するライセンスを残り１回発行可能であることを示している。また、利用条件「ＵＲＵｓ－ＩＤ－１００１１」は、コンテンツＩＤ７０３が「ＣＯＮＴＲＡＣＴ－ＩＤ－９９９９９」なる契約形態に対する利用条件であり、有効期

間７０４は無制限（∞）であり、発行可能なライセンス数も無制限であることを示している。

【００４１】

コンテンツ情報ＤＢ３０４は、コンテンツ毎に設定するライセンス（後述するサブライセンス）を生成するために用いられる、コンテンツ毎の利用条件を格納するデータベースである。

具体的には、コンテンツ情報ＤＢ３０４は、図８に示すコンテンツ情報管理テーブル８００を有し、コンテンツ利用制御システム１内でコンテンツを一意に特定するためのコンテンツＩＤ８０１と、コンテンツ利用制御システム１内でライセンスを一意に特定するためのライセンスＩＤ８０２と、ライセンスが有効である期間を示す有効期間８０３と、ライセンスを利用可能な回数を示す利用可能回数８０４とを管理している。

【００４２】

例えば、図８において、コンテンツＩＤ８０１が「ＣＯＮＴＥＮＴ－ＩＤ－００００１」であるコンテンツは、ライセンスＩＤ８０２が「ＬＩＣＥＮＳＥ－ＩＤ－００００１」、有効期間８０３が「２００３／１２／３１～２００４／１／３０」、利用可能回数８０４が「∞（制限なし）」であることを示しており、これらの値がサブライセンスに設定される。

以上、図３～図８を用いて、データベース部３００の各部についての詳細な説明を行った。

【００４３】

次に、ライセンス処理部３１０の各部についての詳細な説明を行う。ライセンス処理部３１０は、ライセンス発行部３１１、サーバ送受信部３１２とから構成されている。

ライセンス発行部３１１は、端末装置１０２からのライセンス発行要求に応じて、ユーザに対するライセンス（後述するメインライセンス）を生成するための部である。また、コンテンツ鍵Ｋｃ２０５をデジタル放送経由でコンテンツとともに端末装置１０２に送信するため、コンテンツ鍵Ｋｃ２０５を含むライセンス（後述するサブライセンス）を発行し、コンテンツ配信サーバ１０１ｂに送信する処理を行う。

【００４４】

具体的には、ライセンス発行部３１１は、端末装置１０２からのライセンス発行要求を受け、鍵情報ＤＢ３０１のワーク鍵管理テーブル４００と、ユーザ情報ＤＢ３０２と、利用条件ＤＢ３０３とを利用し、ライセンス発行要求がユーザの利用条件を満たすか否かを判定した上で、ユーザの契約に対応するライセンスを生成する処理を行う。ユーザの契約に対して発行され、契約に対応する複数のコンテンツが利用可能なライセンスをメインライセンスと呼び、図２に示したワーク鍵Ｋｗ２０３を含む。

【００４５】

一方、コンテンツ配信サーバ１０１ｂに送信するライセンスは、単一コンテンツに対して発行されるライセンスであり、サブライセンスと呼ばれる。サブライセンスは図２に示したコンテンツ鍵Ｋｃ２０５を含み、ワーク鍵Ｋｗ２０３で暗号化される。また、サブライセンスは、コンテンツ配信サーバ１０１ｂでＥＣＭに設定され、端末装置１０２に送信される。よって、サブライセンスが設定されたコンテンツを利用するためには、サブライセンスを暗号化しているワーク鍵Ｋｗ２０３が設定されたメインライセンスを取得する必要がある。

【００４６】

サーバ送受信部３１２は、ネットワーク１０３を通じて、端末装置１０２と通信するための部である。

以上、権利管理サーバ１０１ａの詳細な構成についての説明を行った。

ここで、ライセンス発行部３１１が生成するメインライセンス、および、サブライセンスについての構成を図９～図１０を用いて詳細に説明する。

【００４７】

図９は、メインライセンスの構成の一例を示す図である。図９に示すメインライセンス

９００は、メインライセンス９００が利用を許諾するコンテンツの集合、すなわち、サブスクリプション（契約）の種類を識別する契約ＩＤやメインライセンス９００の有効期限（契約の有効期限）などを含むライセンスヘッダ９０１、コンテンツの再生や、記録メディアへのコピーなどに関する利用条件を示すアクションタグブロック９０２、暗号化されたコンテンツ鍵Ｋｃ２０５を復号するためのワーク鍵Ｋｗ２０３を含む暗号鍵タグブロック９０３、メインライセンス９００の改ざんを検出するためのハッシュ値であるライセンスフッタ９０４とから構成されている。

【００４８】

ライセンスヘッダ９０１は、メインライセンス９００を識別するためのライセンス識別子９１１、ユーザ毎またはシステム毎でメインライセンス９００を一意に特定可能な識別子であるライセンスＩＤ９１２、メインライセンス９００全体の長さを示すライセンスサイズ９１３、メインライセンス９００が利用可能な期間を示すライセンス有効期間９１４から構成される。

【００４９】

アクションタグブロック９０２は、「再生」、「コピー」、「印刷」などの、コンテンツに対するユーザのアクションを特定するためのアクションＩＤ９２１と、コンテンツの再生、コピーなどを行う部に固有な利用条件を示す利用部固有条件９２２とから構成される。ここで、利用部固有条件９２２とは、端末装置１０２においてコンテンツを利用する機能を提供するコンテンツ利用部の種類や性能に依存する利用条件である。例えば、映画コンテンツの音声チャネルの指定（５．１ｃｈで再生可能か、２ｃｈで再生可能か）や、映像コンテンツの解像度、サイズの指定などが挙げられる。

【００５０】

暗号鍵タグブロック９０３は、ワーク鍵Ｋｗ２０３がバイナリ値で設定され、ＥＣＭ－ＫｗやＫｃ配信用ＥＣＭなどのサブライセンスを含むＥＣＭを復号するために用いられる。

ライセンスフッタ９０４は、メインライセンス９００をハードディスクなどの非セキュアな領域に蓄積する場合に、改ざんの検出を行い、その正当性を確保するためのものであって、メインライセンス９００の内容が更新される度に、メインライセンス９００の改ざんを防止したい箇所についてのハッシュ値を計算し、計算結果を管理する。このハッシュ値は、ハード的に耐タンパされたエリアで管理される必要がある。具体的なハッシュアルゴリズムとしては、ＳＨＡ－１（Ｓｅｃｕｒｅ　Ｈａｓｈ　Ａｌｇｏｒｉｔｈｍ．１）や、ＳＨＡ－２５６などを用いることができる。

【００５１】

一方、図１０はサブライセンスの一例を示す図である。サブライセンス１０００は、メインライセンス９００と比較して、サブライセンス１０００が利用を許諾する単一のコンテンツを指定するため、ライセンスヘッダ９０１にコンテンツＩＤ１０１４が設定できるようになっている。また、アクションタグブロック１００２には、コンテンツの再生や、記録メディアへのコピーが可能な回数などの利用条件を示す回数カウンタ１０２２が存在している。また、暗号鍵タグブロック１００３には、ＥＣＭ－Ｋｃを復号するためのコンテンツ鍵Ｋｃ２０５がバイナリ値で設定される。サブライセンス１０００におけるその他の項目については、メインライセンス９００と同様であるので、ここでは説明を省略する。なお、メインライセンス９００とサブライセンス１０００で同一の項目がある場合は、サブライセンス１０００に設定されている値を適用するものとするが、運用に応じて、どちらのライセンスを優先的に適用するかを決定しても良い。

【００５２】

以上、図９～図１０を用いて、コンテンツ利用制御システム１におけるライセンスであるメインライセンス９００およびサブライセンス１０００について、その詳細な構成の説明を行ったことにより、ライセンス処理部３１０の各々の部についての詳細な説明を終了する。

次に、図１１は、図１に示される配信センター１０１におけるコンテンツ配信サーバ１

０１ｂの詳細な構成を示す機能ブロック図である。

【００５３】

コンテンツ配信サーバ１０１ｂは、ＭＰＥＧ－２、ＭＰＥＧ－４などのコンテンツをＭＰＥＧ－２　ＴＳパケットの形式で出力する装置であって、コンテンツＤＢ１１０１と、コンテンツ属性情報ＤＢ１１０２と、計時部１１０３と、時刻情報付加部１１０４と、コンテンツ符号化部１１０５と、再生制御情報生成部１１０６と、ＥＣＭ生成部１１０７と、コンテンツ多重化部１１０８と、コンテンツ暗号化部１１０９と、コンテンツ送出部１１１０とから構成される。

【００５４】

コンテンツＤＢ１１０１は、コンテンツを蓄積するためのデータベースである。具体的には、コンテンツＤＢ１１０１は、例えば、映画、ドキュメンタリーなどを蓄積するＶＣＲ（Ｖｉｄｅｏ　Ｃａｓｓｅｔｔｅ　Ｒｅｃｏｒｄｅｒ）などであったり、ライブ放送（生放送）時であれば、映像、音声を撮影するためのビデオカメラであったりする。

コンテンツ属性情報ＤＢ１１０２は、コンテンツ名称やコンテンツ中の構成内容など、コンテンツに関する種々の情報を蓄積するためのデータベースである。具体的には、コンテンツ属性情報ＤＢ１１０２は、図１２に示すように、本コンテンツ利用制御システム内でコンテンツを一意に特定するためのコンテンツＩＤ１２０１と、コンテンツ名を示すコンテンツ名称１２０２と、コンテンツがＰＰＶ（Ｐａｙ　Ｐｅｒ　Ｖｉｅｗ）型のコンテンツである場合において、コンテンツ購入前の試聴を許可する区間を示すプレビュー可能区間１２０３と、コンテンツ中に含まれるＣＭ部分を示すＣＭ区間１２０４とを有するコンテンツ属性情報管理テーブル１２００を備えている。

【００５５】

例えば、コンテンツＩＤ１２０１が「ＣＯＮＴＥＮＴ－ＩＤ－００００１」であるコンテンツは、コンテンツ名称１２０２が「井上哲也ＮＥＷＳ２３」であり、プレビュー可能区間１２０３はコンテンツの先頭からの相対値として「０分～１０分」であり、ＣＭ区間１２０４はコンテンツの先頭からの相対値として、「５分～８分」、「２０分～２５分」、「４０分～４３分」という属性を有することを示している。また、コンテンツＩＤ１２０１が「ＣＯＮＴＥＮＴ－ＩＤ－００００２」である「プロダクトＸ」というコンテンツ名称１２０２のコンテンツに関しては、リアルタイム視聴時のプレビュー可能区間（０分～１０分）と、蓄積視聴時のプレビュー可能区間（５分～１０分、２０分～３０分、など）とが異なる属性を有しており、蓄積視聴の特徴を生かしたコンテンツ属性の設定がされている。また、ＣＭ区間１２０４に関しては、ＣＭを含むコンテンツではないため、「－（ＣＭ無し）」となっている。なお、プレビュー可能区間１２０３が設定されていないコンテンツに関しては、プレビューが許可されていないことを示し、ＣＭ区間１２０４が設定されていないコンテンツに関しては、ＣＭが含まれていないコンテンツなので、コンテンツ内で特殊再生を禁止する部分が存在しないことを示している。

【００５６】

計時部１１０３は、コンテンツ配信サーバ１０１ｂ内での基準となる時刻を出力する部である。具体的には、計時部１１０３は、ＳＴＣ（Ｓｙｓｔｅｍ　Ｔｉｍｅ　Ｃｌｏｃｋ）と呼ばれる２７ＭＨｚの精度を有する４２ビットの基準時刻を生成して、時刻情報付加部１１０４に供給する。

時刻情報付加部１１０４は、計時部１１０３から時刻情報を取得し、コンテンツ符号化部１１０５に対して時刻情報を付加する部である。具体的には、時刻情報付加部１１０４は、計時部１１０３からＳＴＣの値を取得して、コンテンツ符号化部１１０５に対して、ＭＰＥＧ－２　Ｓｙｓｔｅｍｓの規約に従い、少なくとも７００ｍｓの精度でＰＴＳ（Ｐｒｅｓｅｎｔａｔｉｏｎ　Ｔｉｍｅ　Ｓｔａｍｐ）およびＤＴＳ（Ｄｅｃｏｄｉｎｇ　Ｔｉｍｅ　Ｓｔａｍｐ）のためのタイムスタンプを付与する。また、ＭＰＥＧ－２　Ｓｙｓｔｅｍｓの規約に従い、少なくとも１００ｍｓの精度でＰＣＲ（Ｐｒｏｇｒａｍ　Ｃｌｏｃｋ　Ｒｅｆｅｒｅｎｃｅ）のためのタイムスタンプを付与する。

【００５７】

なお、ここでは、計時部１１０３および時刻情報付加部１１０４は、次に説明するコンテンツ符号化部１１０５の外部に備える場合の例を示したが、コンテンツ符号化部１１０５の内部に備えるようにしても良い。

コンテンツ符号化部１１０５は、端末装置１０２に送出するコンテンツをコンテンツＤＢ１１０１から読み出し、コンテンツをＭＰＥＧ形式で符号化する部である。

【００５８】

具体的には、コンテンツ符号化部１１０５は、ＭＰＥＧストリームを生成するリアルタイムエンコーダであって、上流システム（例えば、番組運行管理システムなど）の指示により、コンテンツＤＢ１１０１から映像、音声などを読み出し、映像、音声、データなどのＭＰＥＧ－２やＭＰＥＧ－４のＥＳを生成する。さらに、これらのＥＳを含むＰＥＳパケットを生成し、最後にＭＰＥＧ－２　ＴＳパケット化して、コンテンツ多重化部１１０８に送出する。

【００５９】

ここで、図１３を用いて、ＰＥＳパケットの構成の概要について説明する。図１３に示すＰＥＳパケット１３００は、ＰＥＳパケットの開始を示すコードであるＰａｃｋｅｔ　Ｓｔａｒｔ　Ｃｏｄｅ　Ｐｒｅｆｉｘ１３００と、ＰＥＳに含まれる音声、映像などのデータの種類を示すＳｔｒｅａｍ　ｉｄ１３２０と、ＰＥＳパケット１３００の長さを示すＰＥＳ　Ｐａｃｋｅｔ　Ｌｅｎｇｔｈ１３３０と、オプションのＰＥＳヘッダであるＯｐｔｉｏｎａｌ　ＰＥＳ　Ｈｅａｄｅｒ１３４０と、スタッフィングであるＳｔｕｆｆｉｎｇ　Ｂｙｔｅｓ１３５０と、音声、映像などのデータ（ＥＳ）が設定されるＰＥＳ　Ｐａｃｋｅｔ　Ｄａｔａ　Ｂｙｔｅｓ１３６０とから構成される。

【００６０】

また、図１４は、ＴＳパケットの構成の概要を示す図である。ＴＳパケット１４００は、ＴＳパケット１４００の開始を示すコードやＴＳパケットに設定されるデータの種類などを特定するためのＰＩＤ（Ｐａｃｋｅｔ　ＩＤ）、ＴＳパケットのペイロード（後述するＴＳＰ　Ｐａｙｌｏａｄ１４３０）の暗号化の有無を示すフラグであるｔｒａｎｓｐｏｒｔ＿ｓｃｒａｍｂｌｉｎｇ＿ｃｏｎｔｒｏｌなどが含まれるＴＳパケット１４００のヘッダであるＴＳＰ　Ｈｅａｄｅｒ１４１０と、オプション的に用いられ、時刻情報やプライベートデータなどが設定可能なＡｄａｐｔａｔｉｏｎ　Ｆｉｅｌｄ１４２０と、ＰＥＳパケット１４００や、ＰＳＩ／ＳＩなどが設定されるペイロードであるＴＳＰ　Ｐａｙｌｏａｄ１４３０とから構成される。

【００６１】

なお、ＭＰＥＧ－２　ＳｙｓｔｅｍｓのＰＥＳパケットやＴＳパケットについては、国際標準規格であるＩＳＯ／ＩＥＣ　１３８１８－１が詳しい。

図１３および図１４で説明したＰＥＳパケット１３００およびＴＳパケット１４００を用いて、コンテンツ符号化部１１０５が設定する時刻情報について説明する。コンテンツ符号化部１１０５は、時刻情報付加部１１０４から取得した時刻情報、すなわちＳＴＣの値を用いて、ＰＥＳパケット１３００を生成する際、Ｏｐｔｉｏｎａｌ　ＰＥＳ　Ｈｅａｄｅｒ１３４０中の、Ｏｐｔｉｏｎａｌ　Ｆｉｅｌｄｓ１３４３の要素であるＰＴＳ１３４３ａ、ＤＴＳ１３４３ｂをＰＥＳパケット１３００に付加する。

【００６２】

ＰＴＳ１３４３ａは、当該ＰＥＳパケット１３００に含まれる映像、音声などを端末装置１０２ａ～１０２ｃにおいて表示する時刻を示す情報である。また、ＤＴＳ１３４３ｂは、当該ＰＥＳパケット１３００に含まれる映像、音声などをデコードする時刻を示す情報である。

これらのＰＴＳ１３４３ａおよびＤＴＳ１３４３ｂは、端末装置１０２ａ～１０２ｃにおいて、端末装置１０２ａ～１０２ｃが保持するＳＴＣと一致する毎に、個々のＰＥＳパケットのデコード、表示を確実に行えるようにするために、適切なＰＥＳパケット１３００に設定されるものである。

【００６３】

また、コンテンツ符号化部１１０５は、ＴＳパケット１４００を生成する際、時刻情報付加部１１０４から取得した時刻情報（ＳＴＣ）の値を用いて、ＴＳパケット１４００のＡｄａｐｔａｔｉｏｎ　Ｆｉｅｌｄ１４２０のＯｐｔｉｏｎａｌ　Ｆｉｅｌｄｓ１４２５内の要素であるＰＣＲ１４２５ａを付加する。端末装置１０２ａ～１０２ｃは、このＰＣＲ１４２５ａを用いて、複数のＥＳ（映像、音声、データなど）を同期させる際の基準となり、送信装置のＳＴＣと同期した基準クロック（ＳＴＣ）を再生することが可能となる。

【００６４】

以下、図１１に戻って、コンテンツ配信サーバ１０１ｂの構成についての説明を継続する。

再生制御情報生成部１１０６は、コンテンツの特定部分の再生を制御するための情報を生成する部である。具体的には、再生制御情報生成部１１０６は、コンテンツ配信サーバ１０１ｂから送出するコンテンツについて、コンテンツ属性情報ＤＢ１１０２が管理するコンテンツ属性情報管理テーブル１２００から、対応するコンテンツのプレビュー可能区間１２０３およびＣＭ区間１２０４を取得し、再生制御情報として、それぞれに対応するプレビュー制御情報、および、ＣＭスキップ制御情報を生成する。この再生制御情報を、権利管理サーバ１０１ａで生成されたサブライセンス１０００に設定するため、サブライセンス１０００に設定可能な形式である制御情報タグブロックを生成し、制御情報タグブロック中に再生制御情報を設定する。この制御情報タグブロックのデータ構造を図１５に示す。

【００６５】

図１５に示す制御情報タグブロック１５００は、本タグブロックが制御情報タグブロック１５００であることを示す制御情報タグ値１５０１と、制御情報タグブロック１５００のサイズを示す制御情報長１５０２と、プレビュー制御情報やＣＭスキップ制御情報などの再生制御情報を示す制御情報１５０３とから構成されている。

さらに、制御情報１５０３は、制御情報１５０３に含まれる再生制御情報の個数を示す制御情報個数１５１０と、再生制御内容を示す制御ＩＤ１５１１と、再生制御の期限を示す制御期限１５１２と、再生制御を行う回数を示す制御回数１５１３と、再生制御を行うコンテンツの特定箇所をコンテンツに付加された時刻情報を用いて指定する制御範囲１５１４とから構成されている。制御範囲１５１４は、再生制御を行うコンテンツの特定箇所を、制御開始時刻（１５２１、１５２３）と制御終了時刻（１５２２、１５２４）の組を用いて指定している。また、制御範囲１５１４に含まれる制御開始時刻と制御終了時刻の組は、複数個設定される可能性があるため、制御時刻個数１５２０として、制御範囲１５１４に設定された制御開始時刻と制御終了時刻の組の個数を示すようになっている。

【００６６】

このとき、コンテンツ属性情報管理テーブル１２００のプレビュー可能区間１２０３およびＣＭ区間１２０４は、コンテンツの先頭からの相対時刻となっているため、実際にコンテンツに付加される時刻情報（ＰＴＳ１３４３ａ）を用いた値に変換する必要がある。ＰＴＳ１３４３ａは９０ＫＨｚのクロック値であるため、コンテンツの先頭からの相対時刻を９００００で除することによって、コンテンツの先頭からのＰＴＳ１３４３ａに基づく相対時刻に変換することができる。さらに、コンテンツの先頭のＰＴＳ１３４３ａの値を取得することで、コンテンツに付加されたＰＴＳ１３４３ａを用いて、プレビュー可能区間およびＣＭスキップ制御区間を表現することができる。制御範囲１５１４に設定する制御開始時刻と制御終了時刻の組は、このようにＰＴＳ１３４３ａを用いた時刻情報として設定される。

【００６７】

ところで、制御範囲１５１４を含む再生制御情報は、サブライセンス１０００に設定され、さらにＥＣＭに設定されて、コンテンツ配信サーバ１０１ｂから端末装置１０２に配信される。このとき、端末装置１０２での連続するコンテンツのシームレスな再生を実現するため、ＥＣＭはコンテンツが実際に開始する数秒前から送出される。このため、再生

制御情報をコンテンツの符号化、送出前に生成する必要があり、再生制御情報の生成にあたってはコンテンツの先頭のＰＴＳ１３４３ａを計算により求める必要がある。図１６は、コンテンツの先頭のＰＴＳ１３４３ａを計算により求める方法の概念図である。

【００６８】

図１６は、コンテンツ配信サーバ１０１ｂから端末装置１０２に対して、コンテンツが時刻ｔ２に送出開始される場合の例を示している。また、前述したように、コンテンツ配信サーバ１０１ｂではコンテンツの送出開始に先立ち、βだけ前（時刻ｔ１）にＥＣＭを送出する必要がある。このとき、再生制御情報を生成するタイミング（時刻ｔ０）は、再生制御情報やＥＣＭの生成に要する時間αを考慮した上で決定する必要がある。ここで、αは時間Ａ～時間Ｄの和として表すことができ、具体的な時間Ａ～時間Ｄの値として、時間Ａがコンテンツ符号化部１１０５から時刻ｔ０の時点でのＰＴＳの値を取得するのに要する時間、時間Ｂがコンテンツの先頭のＰＴＳの値を算出する時間、時間Ｃが再生制御情報を生成し、サブライセンス１０００に設定するのに要する時間、時間ＤがＥＣＭを生成し、ワーク鍵Ｋｗ２０３、コンテンツ鍵Ｋｃ２０５で暗号化するのに要する時間、となる。すなわち、コンテンツの送出開始時のＰＴＳ１３４３ａの値（コンテンツの先頭のＰＴＳ１３４３ａ）は、時刻ｔ０にコンテンツ符号化部１１０５から取得したＰＴＳ１３４３ａの値に、時間αと時間βを加算した値として算出することができる。

【００６９】

なお、ここでは、制御範囲１５１４として、制御開始時刻と制御終了時刻に算出したＰＴＳ１３４３ａの値をそのまま設定する場合の例を示したが、制御範囲１５１４にはＰＴＳ１３４３ａの値を用いたコンテンツ先頭からの相対時刻を設定しておき、再生制御情報などにコンテンツ先頭のＰＴＳ１３４３ａの値を別途設定するようにしても良い。このようにすることにより、再生制御情報の生成処理（上述した時間Ｃに相当）における時刻情報の演算量を削減することができる。

【００７０】

このように生成した再生制御情報（制御情報１５０３）の例を、図１７に示す。以下では、図１５と図１７とを用いて説明を行う。図１７では、制御情報個数１５１０として「２」となっており、後述するように、プレビュー制御のための情報と、ＣＭスキップ制御のための情報の２つの情報から構成されている。１つめの情報としては、制御ＩＤ１５１１として「プレビュー可」、制御期限１５１２が「２００４／９／１４」、制御回数１５１３が「１回」、制御範囲１５１４が「１００００～１０００００」となっているので、当該コンテンツに関わるプレビュー制御としては、２００４／９／１４までの期間で、プレビューが可能な部分として、ＰＴＳ１３４３ａの値が１００００～１０００００である部分を１回だけプレビューして良いことを示している。ここで、制御回数１５１３に関しては、端末装置１０２でのコンテンツ利用時に、コンテンツ再生箇所のＰＴＳ１３４３ａを視聴履歴として記録し、該当箇所を何回視聴したかを管理することにより実現する。また、２つ目の情報として、制御ＩＤ１５１１が「特殊再生不可」、制御期限１５１２が「２００４／７／６」、制御回数１５１３が「３回」、制御範囲１５１４が「２００００～１０００００」、「５０００００～１０００００」などとなっているので、当該コンテンツのＣＭ部分に関わる特殊再生制御としては、２００４／９／１４までの期間で、ＣＭスキップが不可能な部分として、ＰＴＳ１３４３ａの値が２００００～１０００００、５００００～１０００００などの部分を、少なくとも通常再生で３回視聴するように制御することを示している。

【００７１】

以上のように生成した再生制御情報を含む制御情報タグブロック１５００は、サブライセンス１０００に設定され、さらにＥＣＭに設定されるため、ＥＣＭ生成部１１０７に送信される。なお、再生制御情報を設定するライセンスのＩＤを、再生制御情報中に設定するようにし、どのライセンスに対する再生制御情報かを明確に識別可能なようにしても良い。

【００７２】

以下、再び図１１に戻って、コンテンツ配信サーバ１０１ｂの構成についての説明を継続する。

ＥＣＭ生成部１１０７は、スクランブル鍵Ｋｓ２０１やメインライセンス９００を含むＥＣＭを生成する部である。具体的には、ＥＣＭ生成部１１０７は、権利管理サーバ１０１ａからワーク鍵Ｋｗ２０３、コンテンツ鍵Ｋｃ２０５、サブライセンス１０００を受信するとともに、再生制御情報生成部１１０６から制御情報タグブロック１５００を受信する。上流システムからの指示によりＥＣＭ－Ｋｗ、ＥＣＭ－Ｋｃ、Ｋｃ配信用ＥＣＭを生成し、図１１には図示しないスクランブル鍵生成部において生成したコンテンツのスクランブル鍵Ｋｓ２０１を設定するとともに、制御情報タグブロック１５００をサブライセンス１０００に挿入して、Ｋｃ配信用ＥＣＭに設定する。さらに、生成した各ＥＣＭをワーク鍵Ｋｗ２０３、コンテンツ鍵Ｋｃ２０５により暗号化して、コンテンツ多重化部１１０８に生成したＥＣＭを送信する。また、生成したスクランブル鍵Ｋｓ２０１を、コンテンツを暗号化するコンテンツ暗号化部１１０９に送信する。

【００７３】

ここで、図１８～図１９を用いて、ＥＣＭ－Ｋｗ、ＥＣＭ－Ｋｃ、Ｋｃ配信用ＥＣＭのデータ構造についての詳細な説明を行う。

図１８は、主としてスクランブル鍵Ｋｓ２０１を伝送するＥＣＭのデータ構造の一例を示す図である。端末装置１０２において、リアルタイム視聴用のワーク鍵Ｋｗ２０３で暗号化されたＥＣＭ－Ｋｗ１８００と、蓄積視聴用のコンテンツ鍵Ｋｓ２０５で暗号化されたＥＣＭ－Ｋｃ１８１０のフォーマットは同一であり、暗号化を行う暗号鍵（ワーク鍵Ｋｗ２０３とコンテンツ鍵Ｋｓ２０５）が異なるのみである。

【００７４】

図１８に示したＥＣＭ－Ｋｗ１８００、および、ＥＣＭ－Ｋｃ１８１０は、スクランブル鍵Ｋｓ２０１やコンテンツに関する情報の伝送に用いられる情報であり、事業者ＩＤ１８０２、ワーク鍵ＩＤ１８０３、コンテンツＩＤ１８０４、スクランブル鍵Ｋｓ２０１、コンテンツ関連情報１８０６、改ざん検出１８０７とから構成されている。また、ＭＰＥＧ－２　Ｓｙｓｔｅｍｓのプライベートセクション形式でトランスポートストリームに多重化するため、セクションヘッダ１８０１、セクションテーラ（誤り検出）１８０７が付加されている。

【００７５】

事業者ＩＤ１８０２は、本コンテンツ利用制御システム１において、サービスを提供する事業者を識別するコードであって、次に述べるワーク鍵ＩＤ１８０３とともに参照される。

ワーク鍵ＩＤ１８０３は、ＥＣＭを暗号化するワーク鍵Ｋｗ２０３を識別するための情報であり、ＥＣＭの非暗号化部分に設定される。暗号化されたＥＣＭを復号する場合には、本ワーク鍵ＩＤ１８０３を参照することにより、どのワーク鍵Ｋｗ２０３を用いてＥＣＭを復号すれば良いかを判別することができる。

【００７６】

コンテンツＩＤ１８０４は、コンテンツ毎に割り当てられる識別子であり、本コンテンツ利用制御システム１において、コンテンツを一意に識別するためのコードである。

スクランブル鍵Ｋｓ２０１は、コンテンツのＴＳパケット１４００のペイロード部（ＴＳＰ＿Ｐａｙｌｏａｄ１４３０）を暗号化する暗号鍵である。端末装置１０２が、数秒おきに変更されるスクランブル鍵Ｋｓ２０１を取得するのに要する時間を短縮するため、一般的にはスクランブル鍵２０１に複数の暗号鍵を設定する。

【００７７】

コンテンツ関連情報１８０６は、可変長のデータであり、コンテンツの属性などを示す情報が必要に応じて設定される。

改ざん検出１８０７は、暗号化されるＥＣＭの改ざんを検出するためのハッシュ値が設定される。

次に、図１９は、主として蓄積視聴のためのＥＣＭ－Ｋｃ１８１０を復号するためのコ

ンテンツ鍵Ｋｃ２０５を伝送するＫｃ配信用ＥＣＭのデータ構造の一例を示す図である。

【００７８】

図１９に示したＫｃ配信用ＥＣＭ１９００は、コンテンツ鍵Ｋｃ２０５やサブライセンス１０００の伝送に用いられる情報であり、事業者ＩＤ１９０２、ワーク鍵ＩＤ１９０３、サブライセンス１０００、改ざん検出１９０４とから構成されている。コンテンツ鍵Ｋｃ２０５やコンテンツＩＤは、サブライセンス１０００に含まれる。また、ＥＣＭ－Ｋｗ１８００およびＥＣＭ－Ｋｃ１８１０と同様に、セクションヘッダ１９０１、セクションテーラ（誤り検出）１９０５が付加されている。

【００７９】

事業者ＩＤ１９０２、ワーク鍵ＩＤ１９０３、改ざん検出１９０４については、ＥＣＭ－Ｋｗ１８００およびＥＣＭ－Ｋｃ１８１０における事業者ＩＤ１８０２、ワーク鍵ＩＤ１８０３、改ざん検出１８０８の説明と同様であるので、ここでは説明を省略する。また、サブライセンス１０００については、図２０に示すように、権利管理サーバ１０１ａから取得したサブライセンス１０００に、再生制御情報生成部１００６から取得した制御情報タグブロック１５００を挿入したデータ構造であり、図１０および図１５において、サブライセンス１０００および制御情報タグブロック１５００の各項目については説明済みであるので、ここでは説明を省略する。

【００８０】

なお、ＥＣＭ－Ｋｗ１８００、ＥＣＭ－Ｋｃ１８１０、Ｋｃ配信用ＥＣＭ１９００に時刻情報を含めることもできる。各ＥＣＭは暗号化されて配信されるため、特にリアルタイム視聴においては、ＥＣＭに設定されたセキュアな時刻情報を用いた視聴制御などを行うことができる。

以下、再び図１１に戻って、コンテンツ配信サーバ１０１ｂの構成についての説明を継続する。

【００８１】

コンテンツ多重化部１１０８は、コンテンツ符号化部１１０５から受け取った映像、音声、データなどを含むトランスポートストリームと、ＥＣＭ生成部１１０７から受け取った単数または複数のＥＣＭを含むトランスポートストリームとを多重化し、多重化されたトランスポートストリームをコンテンツ暗号化部１１０９に送出する部である。具体的には、コンテンツ多重化部１１０８は、コンテンツ符号化部１１０５から受信したＴＳパケット化されたコンテンツと、ＥＣＭ生成部１１０７から受信したＴＳパケット化されたＥＣＭ－Ｋｗ１８００、ＥＣＭ－Ｋｃ１８１０、Ｋｃ配信用ＥＣＭ１９００とを多重化して、端末装置１０２に送信するトランスポートストリームを生成する。

【００８２】

コンテンツ暗号化部１１０９は、ＡＥＳなどを用いてコンテンツを暗号化することにより、コンテンツの保護および時刻情報をコンテンツにセキュアにバインドする部である。具体的には、コンテンツ暗号化部９０９は、ＴＳパケットのアダプテーションフィールドを除くペイロード部を、ＥＣＭ生成部１１０７から取得したスクランブル鍵Ｋｓ２０１を用いて、ＣＢＣ（Ｃｉｐｈｅｒ　Ｂｌｏｃｋ　Ｃｈａｉｎｉｎｇ）＋ＯＦＢ（Ｏｕｔｐｕｔ　ＦｅｅｄＢａｃｋ）モードによって暗号化（スクランブル）する。これにより、時刻情報をコンテンツにセキュアにバインドしている。

【００８３】

コンテンツ送出部１１１０は、コンテンツ暗号化部１１０９において暗号化されたＴＳパケット１４００を、端末装置１０２に送出する部である。具体的には、コンテンツ送出部１１１０は、コンテンツ暗号化部１１０９から受け取ったトランスポートストリームを、放送波としてネットワーク１０３を通じて端末装置１０２に送出する。

なお、ここでは、コンテンツＤＢ１１０１に蓄積されたコンテンツを読み出し、コンテンツ符号化部１１０５においてリアルタイムエンコードする場合の例を示したが、あらかじめオフラインでＰＥＳ（ＥＳ）あるいはＴＳを生成しておき、コンテンツＤＢ１１０１に蓄積しておくことにより、コンテンツ送出時にコンテンツ符号化部１１０５におけるエ

ンコード処理を省略するようにしても良い。

【００８４】

また、ここでは、コンテンツＤＢ１１０１に蓄積された非暗号のコンテンツを、コンテンツ暗号化部１１０９で送出時に暗号化する場合の例を示したが、あらかじめ暗号化されたＭＰＥＧ－２　ＴＳコンテンツを格納しておくようにすることもできる。

【００８５】

以上、図１０～図２０を用いて、配信センター１０１から端末装置１０２にコンテンツを送出するコンテンツ配信サーバ１０１ｂの構成についての詳細な説明を行った。また、図２～図２０を用いて、配信センター１０１の各部分についての説明を行った。なお、配信センター１０１における課金サーバ１０１ｃ、ウェブサーバ１０１ｄの詳細な構成については、本発明の主眼ではないため、ここでは省略する。

【００８６】

次に、コンテンツ利用制御システム１における端末装置１０２の構成について説明する。図２１は、図１に示される端末装置１０２の詳細な構成を示す機能ブロック図である。

端末装置１０２は、外部との通信インタフェースを提供する端末送受信部２１０１と、受信したトランスポートストリームをコンテンツとコンテンツ以外のデータとに分離する分離部２１０２と、コンテンツを蓄積するコンテンツ蓄積部２１０３と、ライセンスを処理、管理するライセンス処理部２１０４と、ライセンスを蓄積するライセンスＤＢ２１０５と、セキュアにコンテンツの利用制御を行うコンテンツ利用制御部２１０６と、暗号化コンテンツの復号を行うコンテンツ復号部２１０７と、コンテンツを利用するコンテンツ利用部２１０８と、コンテンツの視聴箇所を視聴履歴として記録する視聴履歴記録部２１０９と、視聴履歴を蓄積する視聴履歴ＤＢ２１１０と、主としてユーザに対してインタフェースを提供する端末アプリケーション２１１１とから構成されている。

【００８７】

端末送受信部２１０１は、ネットワーク１０３を通じて、配信センター１０１と通信するための部である。

分離部２１０２は、ＭＰＥＧ－２　ＴＳにより多重化された暗号化コンテンツを取得し、トランスポートストリームに含まれるＰＡＴ（Ｐｒｏｇｒａｍ　Ａｓｓｏｃｉａｔｉｏｎ　Ｔａｂｌｅ）、ＰＭＴ（Ｐｒｏｇｒａｍ　Ｍａｐ　Ｔａｂｌｅ）などのＰＳＩ情報を参照して、コンテンツの映像、音声、データや、ＥＣＭ－Ｋｗ１８００、ＥＣＭ－Ｋｃ１８１０、Ｋｃ配信用ＥＣＭ１９００を含むＴＳパケット１４００、および、ＰＣＲ１４２５ａが挿入されているＴＳパケット１４００のＰＩＤを取得し、コンテンツとＥＣＭを分離する部である。また、分離部２１０２は、同時に、ＰＭＴに記載されているＰＣＲ＿ＰＩＤ（ＰＣＲが含まれているＰＩＤを示す）を参照することにより、ＴＳパケット１４００のＡｄａｐｔａｔｉｏｎ＿ｆｉｅｌｄ１４２０にＰＣＲ１４２５ａが挿入されているＰＩＤのＴＳパケット１４００を取得して、端末装置１０２でのコンテンツ再生の基準クロックとして、図２１に図示しない計時部に供給する。また、コンテンツ蓄積部２１０３に一旦コンテンツを蓄積する場合には、ＰＡＴ、ＰＭＴなどのＰＳＩ情報から必要な情報を選択してＳＩＴ（Ｓｅｌｅｃｔｉｏｎ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｔａｂｌｅ）、ＤＩＴ（Ｄｉｓｃｏｎｔｉｎｕｉｔｙ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｔａｂｌｅ）などのＰＳＩ情報の生成を行い、受信したトランスポートストリームを、パーシャルトランスポートストリーム（以下、パーシャルＴＳと記述する）と呼ばれるストリームを生成する処理を行う。

【００８８】

コンテンツ蓄積部２１０３は、生成したパーシャルＴＳを蓄積する部である。具体的には、コンテンツ蓄積部２１０３は、大容量ＨＤＤなどで実現され、分離部２１０２において受信したトランスポートストリームから生成したパーシャルＴＳを蓄積する。

ライセンス処理部２１０４は、ライセンスに基づき、セキュアにコンテンツの利用可否判定を行う。具体的には、ライセンス処理部２１０４は、ユーザからコンテンツの利用を要求された場合に、権利管理サーバ１０１ａから取得したメインライセンス９００、ある

いは、コンテンツとともに取得するサブライセンス１０００に含まれる利用条件に基づき、コンテンツの利用が可能かどうかを判定する。そして、利用条件がコンテンツの利用を許諾している場合に限り、暗号化コンテンツを復号するための暗号鍵をコンテンツ利用制御部２１０６に渡す、という処理を行う。

【００８９】

例えば、ライセンス処理部２１０４は、メインライセンス９００のライセンスヘッダ９０１に設定された有効期間９１４を参照し、コンテンツが利用可能であるかどうかを判定する。端末装置１０２に保持している、図２１には図示しないセキュアな計時部により提供される現在時刻を参照し、現在時刻が有効期間９１４内である場合は、コンテンツの再生が可能であると判定するという処理を行う。

【００９０】

なお、ライセンス処理部２１０４とコンテンツ利用制御部２１０６とコンテンツ復号部２１０７との間は、コンテンツ鍵Ｋｃ２０５をセキュアに送受信するため、ＳＡＣを確立して安全にコンテンツ鍵Ｋｃ２０５の送受信が行われる。但し、ライセンス処理部２１０４とコンテンツ利用制御部２１０６とコンテンツ復号部２１０７と、同じシステムＬＳＩ内などの同一耐タンパ領域にある場合は、安全にコンテンツ鍵Ｋｃ２０５の送受信を行うことができるので、必ずしもＳＡＣを確立する必要はない。

【００９１】

ライセンスＤＢ２１０５は、セキュアにライセンスを管理するためのデータベースであり、ライセンス処理部２１０４により取得されたメインライセンス９００などを蓄積する。具体的には、ライセンスＤＢ２１０５は、図９で示される権利管理サーバ１０１ａから取得したメインライセンス９００などを蓄積、管理すると共に、改ざんなどの不正な行為を防止するため、ライセンスＤＢ２１０５中のメインライセンス９００などのハッシュ値を、ハード的またはソフト的に耐タンパ化された領域に格納する。

【００９２】

コンテンツ利用制御部２１０６は、ライセンス処理部２１０４からワーク鍵Ｋｗ２０３と利用条件とを用いて、セキュアにコンテンツの利用を制御するための部である。具体的には、コンテンツ利用制御部２１０６は、リアルタイム視聴時においては、分離部２１０２から受け取ったトランスポートストリームからＥＣＭ－Ｋｗ１８００のＴＳパケット１４００を取得し、ＥＣＭ－Ｋｗ１８００を再構成する。このようにして得られたＥＣＭ－Ｋｗ１８００をワーク鍵Ｋｗ２０３により復号して、コンテンツをデスクランブルするためのスクランブル鍵Ｋｓ２０１を取得し、コンテンツ復号部２１０７に供給する。蓄積視聴時においては、コンテンツ蓄積部２１０３から読み出したトランスポートストリームから、Ｋｃ配信用ＥＣＭ１９００をワーク鍵Ｋｗ２０３により復号して、サブライセンス１０００を取得する。そして、サブライセンス１０００に含まれる利用条件判定を行った上で、コンテンツを利用可能である場合のみ、サブライセンス１０００に含まれるコンテンツ鍵Ｋｃ２０５を用いて、ＥＣＭ－Ｋｃ１８１０を復号して、スクランブル鍵Ｋｓ２０１を取得する。

【００９３】

さらに、コンテンツ利用制御部２１０６は、図２１に図示しないセキュアな計時部を用いて、コンテンツの利用時間などを計時することにより、利用条件に従ったコンテンツ利用を制御する。

コンテンツ復号部２１０７は、暗号化されたコンテンツを復号する部である。具体的には、コンテンツ復号部２１０７は、暗号化されたＭＰＥＧ－２　ＴＳにより多重化されたコンテンツを取得し、トランスポートストリームに含まれるＰＡＴ、ＰＭＴなどのＰＳＩ情報を参照して、コンテンツの映像、音声、データを含むＴＳパケット、および、ＰＣＲが挿入されているＴＳパケットのＰＩＤを取得する。そして、コンテンツ利用制御部２１０６から取得するスクランブル鍵Ｋｓ２０１によって、ＴＳＰ　Ｈｅａｄｅｒ１４１０中のｔｒａｎｓｐｏｒｔ＿ｓｃｒａｍｂｌｉｎｇ＿ｃｏｎｔｒｏｌ（図１４に図示せず）を参照して暗号化されているＴＳパケット１１００のペイロードを復号する。

【００９４】
コンテンツ利用部２１０８は、コンテンツをデコードして、図２１に示さないモニターなどに出力するための部である。具体的には、コンテンツ利用部２１０８は、トランスポートストリーム中のＰＣＲ１４２５ａを取得して、コンテンツ利用部２１０８が有するＰＬＬ（Ｐｈａｓｅｄ　Ｌｏｃｋ　Ｌｏｏｐ）機能により、コンテンツ配信サーバ１０１ｂのＳＴＣ（計時部１１０３）と、コンテンツ利用部２１０８が有するＳＴＣ（図示せず）と同期させる。そして、ＴＳパケット１４００のＴＳＰ　Ｐａｙｌｏａｄ１４３０からＰＥＳパケット１０００のデータを取得して、ＭＰＧＥ－２あるいはＭＰＥＧ－４の映像、音声、データなどのＥＳをデコードして、モニターに出力する。また、コンテンツの利用を終了すると、利用終了通知をコンテンツ利用制御部２１０６に通知する。

【００９５】
視聴履歴記録部２１０９は、コンテンツ利用部２１０８で視聴したコンテンツの視聴箇所の情報を視聴履歴として収集する。具体的には、視聴履歴記録部２１０９は、コンテンツ利用部２１０８で再生開始時および再生終了時のＰＴＳ１３４３ａを取得し、このＰＴＳ１３４３ａの値を視聴履歴として受け取り、ＵＬ（Ｕｓａｇｅ　Ｌｏｇ、以下、ＵＬと記述）として視聴履歴ＤＢ２１１０に蓄積する。ＵＬのデータ構造については、後で図を用いて詳細に説明する。

【００９６】
視聴履歴ＤＢ２１１０は、視聴履歴記録部２１０９により取得されたＵＬを蓄積するデータベースである。ここで、ＵＬのデータ構造について、図２２を用いて説明する。

図２２は、ＵＬの構成の一例を示す図である。ＵＬ２２００をコンテンツ利用制御システム１毎、あるいは、ユーザ毎で一意に特定可能な識別子であるＵＬ識別子２２０１と、ＵＬ２２００全体のサイズを示すＵＬサイズ２２０２と、ＵＬ２２００を生成したユーザを特定するためのユーザＩＤ２２０３と、ＵＬ２２００を生成した端末装置１０２を特定するための端末ＩＤ２２０４と、ユーザが利用したコンテンツとＵＬ２２００とを関連づけるためのコンテンツＩＤ２２０５と、ユーザが利用したライセンス（メインライセンス９００およびサブライセンス１０００）とＵＬ２２００とを関連づけるためのライセンスＩＤ２２０６と、ユーザがコンテンツを操作した内容（種類）を特定するためのアクション種別２２０７と、ユーザがコンテンツの操作開始した絶対時刻である利用開始時刻２２０８と、ＵＬ２２００に設定される時刻情報２２１０の個数を示す時刻情報個数２２０９と、コンテンツ利用部２２０８が取得するコンテンツの利用開始、利用終了時点での時刻情報（ＰＥＳパケット１３００のＰＴＳ１３４３ａ）の値である時刻情報２２１０とから構成されている。

【００９７】
ここで、ライセンスＩＤ２２０６は、例えば、端末装置１０２から権利管理サーバ１０１ａへメインライセンス９００を返却するようなコンテンツ利用制御システムなどの場合、メインライセンス９００とともにＵＬ２２００を収集することにより、ユーザが用いたメインライセンス９００とサブライセンス１０００の対応づけが可能となり、配信センター１０１において視聴履歴とライセンスとを関連づけて管理することができる。

【００９８】
また、アクション種別２２０７は、「再生」、「コピー」、「印刷」などの、コンテンツに対するユーザのアクションを特定するための種別であって、サブライセンス１０００のアクションＩＤ１０２１の値が設定される。ここでは、コンテンツの再生を示す「Ｐｌａｙ」の例が示されている。

さらに、時刻情報２２１０は、ユーザがコンテンツの利用を行った部分を特定するための情報であって、コンテンツの利用開始を表す時刻情報である開始時刻情報と、コンテンツの利用終了を表す時刻情報である終了時刻情報との組が、時刻情報個数２２０９に設定された個数分だけ存在する。ここでは、「開始時刻情報、終了時刻情報」の組がＮ個あり、「開始時刻情報１、終了時刻情報１」が「１３９７０５８４、１３９９９９９９」、「開始時刻情報Ｎ、終了時刻情報Ｎ」が「３２１４１６８３、３９７０５８４３９７０」で

ある場合が示されている。
なお、ＵＬ２２０.0には、ＵＬ２２００の改ざんを検出するためのハッシュ値などは存在していないが、必要に応じて改ざん検出を追加するようにしても良い。

【００９９】

以上、図２２を用いて、端末装置１０２で記録する視聴履歴のデータ構造であるＵＬ２２００について、その詳細な構成について説明を行った。なお、生成したＵＬ２２００を必要に応じて任意のタイミング、もしくは、定期的に配信センター１０１に送信するようにしても良い。

【０１００】

端末アプリケーション２１１１は、権利管理サーバ１０１ａからメインライセンス９００を取得したり、コンテンツの利用開始や終了を指示したりするインタフェースを提供する部である。具体的には、端末アプリケーション２１１１は、ユーザの契約に応じたライセンスの取得要求として、期待ライセンス情報（Ｅｘｐｅｃｔｅｄ　Ｌｉｃｅｎｓｅ　Ｉｎｆｏｒｍａｔｉｏｎ、以下ＥＬＩと記述）を生成し、権利管理サーバ１０１ａに送信することにより、権利管理サーバ１０１ａからライセンスを取得する。

【０１０１】

図２３はＥＬＩの一例を示す図である。ＥＬＩ２３００は、ＥＬＩ識別子２３０１と、端末ＩＤ２３０２と、利用条件ＩＤ２３０３と、契約ＩＤ２３０４とから構成される。ＥＬＩ識別子２３０１には、このデータがＥＬＩ２３００であることを示す情報が記述される。端末ＩＤ２３０２には、ＥＬＩ２３００を生成した端末装置１０２、すなわち、ライセンスを要求する端末装置１０２の端末ＩＤが記述される。利用条件ＩＤ２３０３には、権利管理サーバ１０１ａの利用条件ＤＢ２０３において管理されるユーザの利用条件を特定するための利用条件ＩＤ７０２が記述される。この利用条件ＩＤ７０２は、ユーザが権利管理サーバ１０１ａから利用可能な権利を問い合わせる際のレスポンスで通知される利用条件ＩＤを使用する。契約ＩＤ２３０４は、メインライセンス９００に対応する契約ＩＤを記述する。なお、上記に加えて、ユーザが期待するライセンスの有効期間（メインライセンス９００のライセンスヘッダ９０１に記載される有効期間９１５、またはサブライセンス１０００のライセンスヘッダ１００１に記載される有効期間１０１５）を要求するようにしても良い。

【０１０２】

なお、端末装置１０２のうち、特にセキュリティを必要とするデータを処理する部、具体的には、ライセンス処理部２１０４、ライセンスＤＢ２１０５、コンテンツ利用制御部２１０６、コンテンツ復号部２１０７、コンテンツ利用部２１０８、視聴履歴記録部２１０９、視聴履歴ＤＢ２１１０は、悪意のあるユーザなどによる不正な利用を防止するため、ハードウェア的に耐タンパ化されたシステムＬＳＩや、ソフトウェア的に耐タンパ化されたプログラムなどで実現されるのが一般的である。また、端末装置１０２をコンテンツ利用制御システム１内で一意に特定するためのＩＤ（端末ＩＤ）についても、図２１に図示しない耐タンパ化された場所に保持しているものとする。
以上、図２１～図２３を用いて、端末装置１０２についての詳細な構成の説明を行った。

【０１０３】

さて、以上のように構成された端末装置１０２において、ユーザが配信センター１０１からコンテンツおよびライセンスを取得し、セキュアにコンテンツを利用するとともに、再生制御情報やコンテンツの視聴履歴を用いてコンテンツの視聴をセキュアに制御するという一連の動作を、図２４～図３２に示すフローチャートを用いて説明する。

【０１０４】

なお、ユーザが権利管理サーバ１０１ａからメインライセンス９００を取得するにあたって、事前にウェブサーバ１０１ｄなどを用いたサービスプロバイダへの会員登録、コンテンツの利用条件の購入などの処理が必要であるが、これらの処理については本発明の主眼ではないため、以下の説明では省略する。

最初に、端末装置１０２において、ユーザが権利管理サーバ１０１ａからメインライセンス９００を取得する動作を、図２４に示すフローチャートを用いて説明する。

【０１０５】

まずユーザが、端末アプリケーション２１１１が提供するユーザインタフェースにより、権利管理サーバ１０１ａで管理されているユーザの利用条件（ライセンス）一覧を取得し、利用条件一覧から取得したい契約に対するライセンスを選択すると、端末装置１０２は、メインライセンス９００を権利管理サーバ１０１ａに要求するためのＥＬＩ２３００を作成し、権利管理サーバ１０１ａに送信する（ステップＳ２４０１）。

【０１０６】

具体的には、端末アプリケーション２１１１は、ユーザの契約に対応する契約ＩＤをライセンス処理部２１０４に送信する。ライセンス処理部２１０４は、受け取った契約ＩＤを基に図２３に示したＥＬＩ２３００を生成する。なお、このＥＬＩ２３００に設定する利用条件ＩＤ２３０３は、端末アプリケーション２１１１またはライセンス処理部２１０４が、あらかじめユーザが所有する利用条件を権利管理サーバ１０１ａに直接問い合わせるか、または、ウェブサーバ１０１ｄ経由で問い合わせることにより、利用条件ＩＤ２３０３を取得済みであるものとする。このようにして生成したＥＬＩ２３００を、端末送受信部２１０１を通じて、権利管理サーバ１０１ａに送信する。なお、メインライセンス９００は、その有効期限の間は権利管理サーバ１０１ａから１回だけ取得すれば良い。

【０１０７】

権利管理サーバ１０１ａのライセンス発行部３１１は、サーバ送受信部３１２が端末装置１０２から受信したＥＬＩ２３００を受け取ると、ユーザ情報ＤＢ３０２を参照し、ユーザを特定することにより、ユーザ認証を行う（ステップＳ２４０２）。

具体的には、ユーザ認証は２段階で行なわれる。通常、ライセンスのようなセキュリティを要するデータのやり取りを行う際には、ＳＡＣを確立して安全に通信を行えるようするのが一般的である。よって、第１段階としては、権利管理サーバ１０１ａと端末装置１０２との間でＳＳＬやＴＬＳによりＳＡＣを確立する。この相互認証によって、権利管理サーバ１０１ａは、端末装置１０２が正しい端末ＩＤ２３０２を有することが確認できる。第２段階として、ライセンス発行部３１１が端末ＩＤ２３０２なる端末装置１０２を所有するユーザを特定する。そこでライセンス発行部３１１は、ＥＬＩ２３００に含まれる端末ＩＤ２３０２を取得し、ユーザ情報ＤＢ３０２のユーザ情報管理テーブル６００のユーザＩＤ６０１および端末ＩＤ６０２を参照して、ＥＬＩ２３００に含まれる端末ＩＤ２３０２と一致するユーザ情報管理テーブル６００の端末ＩＤ６０２を検索する。一致する端末ＩＤ６０２が見つかった場合には、関連するユーザＩＤ６０１を取得することができるが、一致する端末ＩＤ６０２が見つからなかった場合には、ユーザ認証は失敗する。

【０１０８】

ライセンス発行部３１１は、ステップＳ２４０２のユーザ認証結果を確認する（ステップＳ２４０３）。

ステップＳ２４０３において、ＹＥＳである場合、すなわち、正しくユーザ認証が行なわれた場合には、メインライセンス９００を発行するための利用条件の確認を行うため、ステップＳ２４０４を実行する。

【０１０９】

ステップＳ２４０３において、ＮＯである場合、すなわち、正しくユーザ認証が行なわれなかった場合には、ライセンス発行不可と判定され、ライセンス発行部３１１はライセンス発行不可通知を端末装置１０２に送信する。

ライセンス発行部３１１は、ライセンス発行可否判定処理を実行する（ステップＳ２４０４）。このライセンス発行可否判定処理については、後で図２４を用いて詳細に説明する。

【０１１０】

ライセンス発行部３１１は、ライセンス発行可否判定処理の結果を参照し、メインライセンス９００が発行可能か否かを判定する（ステップＳ２４０５）。

ステップＳ２４０５において、ＹＥＳである場合、すなわち、ライセンス発行可能と判定された場合には、ステップＳ２４０６を実行する。

ステップＳ２４０５において、ＮＯである場合、すなわち、ライセンス発行不可と判定された場合には、ライセンス発行部３１１はライセンス発行不可通知を端末装置１０２に送信する。

【０１１１】

ライセンス発行部３１１は、メインライセンス９００を生成する（ステップＳ２４０６）。具体的には、ライセンス発行部３１１は、ＥＬＩ２３００および利用条件ＤＢ３０３の利用条件管理テーブル７００を参照するとともに、鍵情報ＤＢ３０１のワーク鍵管理テーブル４００から、契約ＩＤ２２０４（契約ＩＤ４０１）に対応するワーク鍵Ｋｗ２０３を取得し、ＥＬＩ２３００により要求されたメインライセンス９００を生成する。

【０１１２】

ライセンス発行部３１１は、利用条件ＤＢ３０３の利用条件管理テーブル７００を更新する（ステップＳ２４０７）。具体的には、ライセンス発行部３１１は、発行したメインライセンス９００に含まれる利用条件の分だけ、当該ユーザの利用条件を減算する処理を行う。例えば、利用条件管理テーブル７００において、ユーザＩＤ７０１が「ＵＳＥＲ－ＩＤ－００００３」、利用条件ＩＤ７０２が「ＵＲＵｓ－ＩＤ－２４０２４」の利用条件に対するメインライセンス９００の発行を要求された場合、発行可能残回数７０５が「２」であるので、利用条件管理テープ７００の発行可能残回数７０５を「１」に更新するという処理を行う。

【０１１３】

ライセンス発行部３１１は、ステップＳ２４０６において生成したメインライセンス９００を端末装置１０２に送信する（ステップＳ２４０８）。具体的には、ライセンス発行部３１１は、サーバ送受信部３１２を通じて、端末装置１０２にメインライセンス９００を送信する処理を行う。

端末装置１０２のライセンス処理部２１０４は、権利管理サーバ１０１ａから受信したメインライセンス９００を受け取り、メインライセンス９００をライセンスＤＢ２１０５に登録する（ステップＳ２４０９）。具体的には、ライセンス処理部２１０４は、端末送受信部２１０１を通じて、ステップＳ２４０１で生成したＥＬＩ２３００に対するレスポンスとしてメインライセンス９００を取得し、メインライセンス９００をライセンスＤＢ２１０５に書き込み、ライセンスＤＢ２１０５のハッシュ値を更新する。

【０１１４】

なお、ステップＳ２４０３またはステップＳ２４０５において、メインライセンス９００が発行不可であるためにライセンス発行不可通知が送信された場合、端末装置１０２のライセンス処理部２１０４は、ライセンス発行不可通知を受信する（ステップＳ２４１０）。具体的には、端末装置１０２のライセンス処理部２１０４は、権利管理サーバ１０１ａからのライセンス発行不可通知を受信し、端末アプリケーション２１１１のユーザインタフェースを通じて、ユーザにその旨を通知して、本処理を終了する。

【０１１５】

ここで、ステップＳ２４０４のライセンス発行可否判定処理について、図２５を用いて説明する。

まず、ライセンス発行部３１１は、ＥＬＩ２３００で指定された利用条件ＩＤ２２０３が利用条件ＤＢ３０３の利用条件管理テーブル７００に存在するかどうかを確認する（ステップＳ２５０１）。具体的には、ライセンス発行部３１１は、端末装置１０２から受信したＥＬＩ２３００を参照し、利用条件ＩＤ２２０３を取得する。この利用条件ＩＤ２２０３が、利用条件管理テーブル７００中の利用条件ＩＤ７０２と一致するものがあるかどうかを確認する。

【０１１６】

ステップＳ２５０１において、ＹＥＳである場合、すなわち、利用条件管理テーブル７００にＥＬＩ２３００の利用条件ＩＤ２２０３と一致する利用条件ＩＤ７０２が存在する

場合には、さらに、利用条件ＩＤ７０２を有するユーザＩＤ７０１が、図２４におけるステップＳ２４０２で認証に成功した、ユーザ情報ＤＢ３０２のユーザ情報管理テーブル６００中のユーザＩＤ６０１と一致するかどうかを確認する。ここで当該ユーザＩＤが一致した場合には、ステップＳ２５０２を実行し、当該ユーザＩＤが一致しない場合には、ステップＳ２５０５を実行する。

【０１１７】

ステップＳ２５０１において、ＮＯである場合、すなわち、利用条件管理テーブル７００にＥＬＩ２３００の利用条件ＩＤ２２０３と一致する利用条件ＩＤ７０２が存在しない場合には、ステップＳ２５０５を実行する。

次に、ライセンス発行部３１１は、ユーザの利用条件が、有効期限を満たしているかどうかを判定する（ステップＳ２５０２）。具体的には、ライセンス発行部３１１は、利用条件ＤＢ３０３の利用条件管理テーブル７００中の有効期間７０４を参照するとともに、セキュアな計時部（図２に図示せず）から現在時刻を取得し、現在時刻が有効期間７０４で示される開始日時から終了日時の間に含まれているか否かを判定する。

【０１１８】

例えば、利用条件管理テーブル７００中の有効期間７０４が「２００２／１２／２０　１２：１２：１２」である場合に、現在時刻が「２００２／１２／１８　１２：３４：５６」であれば、ユーザの利用条件が有効期限内であると判定し、現在時刻が「２００２／１２／３１　１９：００：００」であれば、ユーザの利用条件は有効期限外であると判定する。

【０１１９】

ステップＳ２５０２において、ＹＥＳである場合、すなわち、ユーザの利用条件が有効期限内である場合には、ステップＳ２５０３を実行する。

ステップＳ２５０２において、ＮＯである場合、すなわち、ユーザの利用条件が有効期限外である場合には、ステップＳ２５０５を実行する。

ライセンス発行部３１１は、ライセンスの発行可能回数が残っているかどうかを判定する（ステップＳ２５０３）。具体的には、ライセンス発行部３１１は、利用条件管理テーブル７００の発行可能残回数７０５が１以上であるかどうかを確認する。例えば、利用条件管理テーブル７００の発行可能残回数が「２」である場合には、ライセンスが発行可能であると判定し、「０」である場合には、ライセンスが発行不可であると判定する。

【０１２０】

ステップＳ２５０３において、ＹＥＳである場合、発行可能残回数７０５が１以上である場合には、ステップＳ２５０４を実行する。

ステップＳ２５０３において、ＮＯである場合、すなわち、発行可能残回数７０５が０である場合には、ステップＳ２５０５を実行する。

ライセンス発行部３１１は、メインライセンス９００が発行可能と判定して、ライセンス発行可否判定処理を終了する（ステップＳ２５０４）。

【０１２１】

また、ステップＳ２５０１～ステップＳ２５０３において、ＮＯである場合、すなわち、ライセンス発行部３１１がメインライセンス９００を発行不可能と判定した場合には、ライセンス発行可否判定処理を終了する（ステップＳ２５０５）。

以上、図２５を用いて、ライセンス発行可否判定処理の説明を行った。

次に、権利管理サーバ１０１ａにおける、サブライセンス１０００の生成処理、および、ワーク鍵Ｋｗ２０３、コンテンツ鍵Ｋｃ２０５、サブライセンス１０００のコンテンツ配信サーバ１０１ｂへの送信処理について、図２６を用いて説明する。

【０１２２】

権利管理サーバ１０１ａは、コンテンツ配信サーバ１０１ｂからのワーク鍵Ｋｗ２０３、コンテンツ鍵Ｋｃ２０５、および、サブライセンス１０００の要求を、ＬＡＮ１０１ｎを通じて図３に図示しない要求受信部で受信すると、ライセンス発行部３１１は、データベース部３００のコンテンツ情報ＤＢ３０４から、対応するコンテンツに関する情報を取

得する（ステップＳ２６０１）。具体的には、ライセンス発行部３１１は、コンテンツ配信サーバ１０１ｂからの要求に含まれるコンテンツＩＤに基づき、コンテンツ情報ＤＢ３０４のコンテンツ情報管理テーブル８００から、サブライセンス１０００を生成するために必要な利用条件として、ライセンスＩＤ８０２、有効期間８０３、利用可能回数８０４を取得する。

【０１２３】

ライセンス発行部３１１は、データベース部３００の鍵情報ＤＢ３０１から、契約に対応するワーク鍵Ｋｗ２０３およびコンテンツにコンテンツ鍵Ｋｃ２０５を取得する（ステップＳ２６０２）、具体的には、ライセンス発行部３１１は、コンテンツ配信サーバ１０１ｂからの要求に含まれる契約ＩＤおよびコンテンツＩＤに基づき、鍵情報ＤＢ３０１のワーク鍵管理テーブル４００およびコンテンツ鍵管理テーブル５００から、契約ＩＤ４０１およびコンテンツＩＤ５０１に一致するワーク鍵Ｋｗ２０３およびコンテンツ鍵Ｋｃ２０５を取得する。なお、ワーク鍵管理テーブル４００およびコンテンツ鍵管理テーブル５００中に、コンテンツ配信サーバ１０１ｂからの要求に対応する契約ＩＤ４０１およびコンテンツＩＤ５０１が存在しない場合については、図２６には示していないが、この場合は、エラーとしてコンテンツ配信サーバ１０１ｂにその旨を通知する処理を行う。

【０１２４】

ライセンス発行部３１１は、サブライセンス１０００を生成する（ステップＳ２６０３）。具体的には、ライセンス発行部３１１は、コンテンツ情報ＤＢ３０４のコンテンツ情報管理テーブル８００から取得した該当コンテンツの利用条件と、鍵情報ＤＢ３０１のコンテンツ鍵管理テーブル５００から取得した該当コンテンツのコンテンツ鍵Ｋｃ２０５とを用いて、図１０に示したサブライセンスを生成する。

【０１２５】

ライセンス発行部３１１は、生成したサブライセンス１０００と、ワーク鍵Ｋｗ２０３、コンテンツ鍵Ｋｃ２０５をコンテンツ配信サーバ１０１ｂに送信する（ステップＳ２６０４）。具体的には、ライセンス発行部３１１は、ステップＳ２６０３において生成したサブライセンス１０００と、鍵情報ＤＢ３０１のワーク鍵管理テーブル４００から取得したワーク鍵Ｋｗ２０３と、鍵情報ＤＢ３０１のコンテンツ鍵管理テーブル５００から取得したコンテンツ鍵Ｋｃ２０５とを、ＬＡＮ１０１ｎを通じてコンテンツ配信サーバ１０１ｂに送信する。

【０１２６】

次に、コンテンツ配信サーバ１０１ｂのＥＣＭ生成処理、および、コンテンツ送信処理について、図２７を用いて説明する。

コンテンツ配信サーバ１０１ｂにおいて、再生制御情報生成部１１０６は、コンテンツ送出指示により、コンテンツ符号化部１１０５から現在のＰＴＳ１３４３ａを取得し、コンテンツの先頭のＰＴＳ１３４３ａの値を算出する（ステップＳ２７０１）。具体的には、再生制御情報生成部１１０６は、番組運行管理システムなどの図１１に図示しない上流システムからのコンテンツ送出指示を受けると、コンテンツ符号化部１１０５から、この時点でのＰＴＳ１３４３ａの値、すなわち、時刻情報付加部１１０４により設定されたＳＴＣの値を取得する。このように取得したＰＴＳ１３４３ａの値（図１６における時刻ｔ０）を用いて、図１６において説明した方法により、コンテンツの先頭でのＰＴＳ１３４３ａの値（図１６における時刻ｔ２）を算出し、これを内部で保持する。

【０１２７】

再生制御情報生成部１１０６は、コンテンツ属性情報ＤＢ１１０２の情報に基づいて再生制御情報を生成して、ＥＣＭ生成部１１０７に送信する（ステップＳ２７０２）。具体的には、再生制御情報生成部１１０６は、コンテンツ属性ＤＢ１１０２のコンテンツ属性情報管理テーブル１２００を参照し、該当するコンテンツＩＤ１２０１のプレビュー可能区間１２０３およびＣＭ区間１１０４を取得して、必要に応じてプレビュー制御のための再生制御情報やＣＭスキップ制御のための再生制御情報を生成する。このとき、ステップＳ２７０１で算出したコンテンツの先頭でのＰＴＳ１３４３ａの値を用いて、コンテンツ

属性情報管理テーブル１２００での時刻情報の記述を、ＰＴＳ１３４３ａを用いた記述に変換する。

【０１２８】

コンテンツ送出部１０１０は、コンテンツの送出が完了したか否かを判定する（ステップＳ２７０３）。具体的には、コンテンツ送出部１１１０は、コンテンツの全てをＴＳパケット１４００として端末装置１０２に送出したか否かを判定する。

ステップＳ２７０３において、ＮＯである場合、すなわち、コンテンツの送出が完了していない場合には、ステップＳ２７０４を実行する。

【０１２９】

ステップＳ２７０３において、ＹＥＳである場合、すなわち、コンテンツの送出が全て完了した場合には、その旨をコンテンツ符号化部１１０５や再生制御情報生成部１１０６、あるいは、上流システムなどに通知して、本処理を終了する。

ＥＣＭ生成部１１０７は、再生制御情報生成部１１０６から受信する再生制御情報と、権利管理サーバ１０１ａから受信するサブライセンス１０００、ワーク鍵Ｋｗ２０３、コンテンツ鍵Ｋｃ２０５とを用いて、ＥＣＭを生成、暗号化して、生成したＥＣＭをコンテンツ多重化部１１０８に送信する（ステップＳ２７０４）。具体的には、ＥＣＭ生成部１１０７は、図１８に示した事業者ＩＤ１８０１やコンテンツ関連情報１８０６など、ＥＣＭを生成するために必要な情報をデータベース（図１１に示さず）などから取得し、平文のＥＣＭ－Ｋｗ１８００、ＥＣＭ－Ｋｃ１８１０を生成して、権利管理サーバ１０１ａから受信した、対応するワーク鍵Ｋｗ２０３、コンテンツ鍵Ｋｃ２０５で暗号化して、暗号化されたＥＣＭ－Ｋｗ１８００、ＥＣＭ－Ｋｃ１８１０を生成する。また、再生制御情報生成部１１０６から取得した再生制御情報（制御情報タグブロック１５０３）を、権利管理サーバ１０１ａから受信したサブライセンス１０００に設定して、事業者ＩＤ１９０１などを用いて平文のＫｃ配信用ＥＣＭ１９００を生成する。平文のＫｃ配信用ＥＣＭ１９００に対して、ワーク鍵Ｋｗ２０３を用いて暗号化することにより、暗号化されたＫｃ配信用ＥＣＭ１９００が生成される。このように生成されたＥＣＭ－Ｋｗ１８００、ＥＣＭ－Ｋｃ１８１０、および、Ｋｃ配信用ＥＣＭ１９００は、ＴＳパケット化された後、コンテンツ多重化部１１０８に送信される。

【０１３０】

また、ＥＣＭ生成部１１０７は、内部で生成し、数秒おきに更新されるスクランブル鍵Ｋｓ２０１を、暗号化すべきＴＳパケット１４００のＰＩＤとともに、順次コンテンツ暗号化部１１０９に送信する処理を行う。

コンテンツ符号化部１１０５は、コンテンツＤＢ１１０１から、該当コンテンツＩＤのコンテンツを読み出す（ステップＳ２７０５）。具体的には、コンテンツ符号化部１１０５は、上流システム（図１１に図示せず）から受け取ったコンテンツＩＤをキーとしてコンテンツＤＢ１１０１を検索し、該当コンテンツを順次読み出す処理を行う。

【０１３１】

コンテンツ符号化部１１０５は、コンテンツＤＢ１１０１から読み出したコンテンツをエンコードして、ＰＥＳパケット１３００、ＴＳパケット１４００を順次生成するとともに、時刻情報を付加する（ステップＳ２７０６）。具体的には、コンテンツ符号化部１１０５は、ステップＳ２７０５においてコンテンツＤＢ１１０１から読み出したコンテンツの映像、音声などを順次ＭＰＥＧエンコードし、時刻情報付与部１１０４から取得したＳＴＣを用いて、映像ＥＳ、音声ＥＳの同期を実現するためのＰＴＳ１３４３ａ、ＤＴＳ１３４３ｂを付与する。さらに、ＰＥＳパケット１３００をＴＳパケット化するとともに、時刻情報付与部１１０４から取得したＳＴＣを用いて、端末装置１０２内の基準クロックを、コンテンツ配信サーバ１０１ｂの基準クロック（計時部１００３）と同期させるためのＰＣＲ１４２５ａを付与する。

【０１３２】

コンテンツ多重化部１１０８は、コンテンツとＥＣＭなどを多重化して、コンテンツ暗号化部１１０９に送信する（ステップＳ２７０７）。具体的には、コンテンツ多重化部１

１０８は、コンテンツ符号化部１１０５から取得したコンテンツのＴＳパケット１４００と、ＥＣＭ生成部１１０７から取得したＥＣＭ－Ｋｗ１８００、ＥＣＭ－Ｋｃ１８１０、Ｋｃ配信用ＥＣＭ１９００のＴＳパケット１４００とを多重化することにより、コンテンツと関連する情報が多重化されたトランスポートストリームを生成する。このとき、コンテンツ多重化部１１０８は、ＰＳＩ（ＰＡＴ、ＰＭＴなど）、ヌルパケットなどのその他のＴＳパケット１４００も生成し、コンテンツやＥＣＭのＴＳパケット１４００と共に多重する。また、必要に応じてＰＣＲ１４２５ａの補正を行う。このように生成したトランスポートストリームを、コンテンツ暗号化部１１０９に送信する。

【０１３３】

コンテンツ暗号化部１１０９においてトランスポートストリームをスクランブルした後、コンテンツ送出部１１１０からトランスポートストリームを送信する（ステップＳ２７０８）。具体的には、コンテンツ暗号化部１１０９は、コンテンツ多重化部１１０８から受信したトランスポートストリームに対し、ＥＣＭ生成部１１０７から取得したスクランブルすべき映像、音声などのＰＩＤを用いて、ＴＳパケット１４００のペイロード部（ＴＳＰ　Ｐａｙｌｏａｄ１４３０）をＥＣＭ生成部１１０７から順次取得するスクランブル鍵Ｋｓ２０１でスクランブルする。

【０１３４】

また、コンテンツ送出部１１１０は、コンテンツ暗号化部１１０９から受け取った暗号化されたＴＳパケット１４００を、順次端末装置１０２に伝送する。その後、ステップＳ２７０３を実行する。

以上、コンテンツ配信サーバ１０１ｂにおけるコンテンツの送出を行う動作についての説明を終了する。

【０１３５】

次に、端末装置１０２において、ユーザがコンテンツ蓄積部２１０３に蓄積されたコンテンツを蓄積視聴する動作を、図２８に示すフローチャートを用いて説明する。

まずユーザは、端末アプリケーション２１１１を通じて、コンテンツ一覧から利用したいコンテンツを選択する。コンテンツ利用制御部２１０６に通知された該当コンテンツに対応するライセンスＩＤが、ライセンス処理部２１０４に送信される（ステップＳ２８０１）。具体的には、コンテンツ利用制御部２１０６は、ユーザが選択したコンテンツＩＤおよびコンテンツの位置を示すＵＲＩ（Ｕｎｉｆｉｅｄ　Ｒｅｓｏｕｒｃｅ　Ｉｄｅｎｔｉｆｉｅｒ）を端末アプリケーション２１１１から受け取り、端末装置１０２が保持するコンテンツに関するメタデータなどを用いて、コンテンツＩＤに対するライセンスＩＤを取得する。このとき、当該コンテンツＩＤがサブスクリプションコンテンツであり、何らかの契約ＩＤと関連付けられている場合には、当該契約ＩＤに対応するライセンスＩＤを取得する。このように取得したライセンスＩＤをライセンス処理部２１０４に送信することにより、該当コンテンツの利用を要求する。

【０１３６】

ライセンス処理部２１０４は、ライセンスＤＢ２１０５から、該当ライセンスＩＤに対応するライセンスを取得する（ステップＳ２８０２）。具体的には、ライセンス処理部２１０４は、コンテンツ利用制御部２１０６から受信したライセンスＩＤをキーとしてライセンスＤＢ２１０５を検索する。

ライセンス処理部２１０４は、ステップＳ２８０２において検索したライセンスを取得し、利用可能なライセンスであるか否かを判定する（ステップＳ２８０３）。具体的には、ライセンス処理部２１０４は、まず、コンテンツ利用制御部２１０６から指定されたライセンスＩＤを有するライセンスが、ライセンスＤＢ２１０５に存在するかどうかを確認する。該当ライセンスが存在する場合には、ライセンスの有効期間などを参照し、ライセンスの有効性を確認する。なお、有効期間の有効性の確認については、端末装置１０２内のセキュアな計時部（図２１に図示せず）から取得した時刻情報を用いて確認するものとする。なお、コンテンツ利用制御部２１０６から指定されたライセンスＩＤに対応するライセンスがライセンスＤＢ２１０６に存在しない場合は、ステップＳ２８０７を実行する

。

【０１３７】

ステップＳ２８０３において、ＹＥＳである場合、すなわち、ライセンスが利用可能であると判定された場合には、ステップＳ２８０４を実行する。

ステップＳ２８０３において、ＮＯである場合、すなわち、ライセンスが利用不可能であると判定された場合には、ステップＳ２８０７を実行する。

ライセンス処理部２１０４は、メインライセンス９００を取得し、ワーク鍵Ｋｗ２０３を取得する（ステップＳ２８０４）。具体的には、ライセンス処理部２１０４は、メインライセンス９００の暗号鍵タグブロック９０３に設定されたワーク鍵Ｋｗ２０３を取得し、内部で保持する。

【０１３８】

ライセンス処理部２１０４は、Ｋｃ配信用ＥＣＭ１９００に含まれるサブライセンス１０００を取得することにより、コンテンツ鍵Ｋｃ２０５および再生制御情報を取得して、コンテンツ利用制御部２１０６に送信する（ステップＳ２８０５）。具体的には、ライセンス処理部２１０４は、分離部２１０２で分離されたＫｃ配信用ＥＣＭ１９００を取得すると、メインライセンス９００から得られたワーク鍵Ｋｗ２０３により、暗号化されたＫｃ配信用ＥＣＭ１９００を復号する。Ｋｃ配信用ＥＣＭ１９００に含まれるサブライセンス１０００を取得すると、ステップＳ２８０３で示したメインライセンス９００の有効性判定と同様な方法によりサブライセンス１０００の有効性を確認した上で、サブライセンス１０００の暗号鍵タグブロック１００３に含まれるコンテンツ鍵Ｋｃ２０５を取得する。また、制御情報タグブロック１５００に含まれる再生制御情報（制御情報１５０３）を取得する。このように取得したコンテンツ鍵Ｋｃ２０５および再生制御情報を、必要に応じてＳＡＣを確立し、コンテンツ利用制御部２１０６に送信する。なお、コンテンツ鍵Ｋｃ２０５は、コンテンツのスクランブル鍵Ｋｓ２０１を取得するため、コンテンツ復号部２１０７に送信される。

【０１３９】

コンテンツ復号部２１０７およびコンテンツ利用部２１０８は、コンテンツ利用制御部２１０６が取得したコンテンツ鍵Ｋｃ２０５および再生制御情報に基づき、セキュアにコンテンツの利用を行う（ステップ２８０６）。

なお、ステップＳ２８０３において、利用可能なライセンスが存在しない場合には、コンテンツ利用制御部２１０６は、ライセンス処理部２１０４から利用不可通知を受信する（ステップＳ２８０７）。コンテンツ利用制御部２１０６は、端末アプリケーション２１１１が提供するユーザインタフェース部を通じて、ユーザにその旨を通知する。

【０１４０】

ここで、ステップＳ２８０６のコンテンツ利用処理について、図２９を用いて説明する。

コンテンツ利用制御部２１０６は、コンテンツの受信を端末送受信部２１０１に指示し、コンテンツ配信サーバ１０１ｂから当該コンテンツを受信する（ステップＳ２９０１）。具体的には、コンテンツ利用制御部２１０６は、端末アプリケーション２１１１から受信したコンテンツのＵＲＩ（デジタル放送の場合はチャネルに相当）を基に、コンテンツ配信サーバ１０１ｂから送信されたコンテンツを受信する。

【０１４１】

コンテンツ利用制御部２１０６は、コンテンツの再生が完了したかどうかを判定する（ステップＳ２９０２）。具体的には、コンテンツ利用制御部２１０６は、端末アプリケーション２１１１からコンテンツ再生終了指示が送信された場合や、コンテンツ配信サーバ１０１ｂからのコンテンツ受信が完了したか否か、もしくは、コンテンツの切れ目（変わり目）をＰＳＩ／ＳＩなどを用いて検出したりすることにより、コンテンツの再生が完了したかどうかを判定する。

【０１４２】

ステップＳ２９０２において、ＮＯである場合、すなわち、コンテンツの再生が完了し

ていない場合には、ステップＳ２９０４を実行する。
ステップＳ２９０２において、ＹＥＳである場合、すなわち、ユーザから端末アプリケーション２１１１を通じて、コンテンツ再生終了の通知を受けた場合や、コンテンツの受信が完了した場合には、端末アプリケーション２１１１を通じてその旨をユーザに通知し、本処理を終了する。

【０１４３】

コンテンツ復号部２１０７は、ＥＣＭ－Ｋｃ１８１０のＴＳパケット１４００を取得して、スクランブル鍵Ｋｓ２０１を取得する（ステップＳ２９０３）。具体的には、コンテンツ復号部２１０７は、分離部２９０２から受信したＥＣＭ－Ｋｃ１８１０のＴＳパケット１４００からＥＣＭ－Ｋｃ１８１０を再構成して、コンテンツ利用制御部２１０６から取得したコンテンツ鍵Ｋｃ２０５を用いて、暗号化されたＥＣＭ－Ｋｃ１８１０を復号し、スクランブル鍵Ｋｓ２０１を取得して内部レジスタなどに保持する。

【０１４４】

コンテンツ復号部２１０７は、コンテンツのＴＳパケット１４００を取得して、内部レジスタに保持したスクランブル鍵Ｋｓ２０１を用いてＴＳパケット１４００のデスクランブルを行い、再構成したコンテンツのデコードを実行する（ステップＳ２９０４）。具体的には、コンテンツ復号部２１０７は、ＴＳＰ　Ｈｅａｄｅｒ１４１０中のｔｒａｎｓｐｏｒｔ＿ｓｃｒａｍｂｌｉｎｇ＿ｃｏｎｔｒｏｌを参照することによって、ペイロード部（ＴＳＰ　Ｐａｙｌｏａｄ１４３０）が暗号化されているＴＳパケット１４００を、スクランブル鍵Ｋｓ２０１を用いてデスクランブルし、デスクランブルされたＴＳパケット１４００を順次コンテンツ利用部２１０８に送信する。コンテンツ利用部２１０８は、コンテンツ復号部２１０７から復号されたＴＳパケット１４００を受信し、ＴＳパケット１４００のペイロード部（ＴＳＰ　Ｐａｙｌｏａｄ１４３０）から復号されたＰＥＳパケット１３００を取得し、コンテンツの映像ＥＳ、音声ＥＳなどのデータを取得して、それぞれのＥＳをデコードして、映像、音声の同期をとりつつ、図２１に示さないモニターなどに出力する。このとき、コンテンツ利用部２１０８は、ＴＳパケット１４００のＡｄａｐｔａｔｉｏｎ　Ｆｉｅｌｄ１４２０のＰＣＲ１４２５ａを取得し、コンテンツ利用部２１０８の内部に有するＳＴＣを、ＰＬＬ（図１５に図示せず）を用いることにより、安定したクロックに保つ処理を行う。よって、このＳＴＣの値と、ＰＥＳパケット１３００のＰＴＳ１３４３ａ、ＤＴＳ１３４３ｂが一致したときにＰＥＳパケット１３００のＰＥＳ　Ｐａｃｋｅｔ　Ｄａｔａ　Ｂｙｔｅｓ１３６０の映像ＥＳ、音声ＥＳなどのデコード、表示を行うことにより、正常なコンテンツ再生を実現する。

【０１４５】

視聴履歴記録部２１０９は、コンテンツ利用部２１０８で表示したコンテンツのＰＴＳ１３４３ａを取得して、視聴履歴ＤＢ２１１０に記録する（ステップＳ２９０５）。具体的には、視聴履歴記録部２１０９は、コンテンツ利用部２１０８がコンテンツを再生した時点のＰＴＳ１３４３ａの値（表示したＰＥＳパケット１３００に含まれるＰＴＳ１３４３ａ）をコンテンツ利用部２１０８から取得し、少なくともコンテンツの再生開始および再生終了時点でのＰＴＳ１３４３ａの値を視聴履歴として視聴履歴ＤＢ２１１０に記録する。なお、ＰＴＳ１３４３ａの記録は、視聴履歴ＤＢ２１１０のデータベース処理負荷を低減するため、表示したＰＴＳ１３４３ａの値を随時内部メモリに保持、更新しておき、適当なタイミングで視聴履歴ＤＢ２１１０をアップデートするようにしても良い。また、セキュアな計時部（図２１に図示せず）から取得した日時情報、ユーザが指示したアクションである「Ｐｌａｙ（再生）」、再生を行ったユーザＩＤや端末ＩＤをともに記録することにより、図２２で示したＵＬ２２００が生成され、視聴履歴ＤＢ２１１０に蓄積される。

【０１４６】

なお、リアルタイム視聴時における端末装置１０２の動作については、図２８で説明したステップＳ２８０５において、コンテンツ鍵Ｋｃ２０５の代わりにワーク鍵Ｋｗ２０３を取得し、ワーク鍵Ｋｗ２０３を用いてＥＣＭ－Ｋｗ１８００を復号することによりスク

ランブル鍵Ｋｓ２０１が得られる点が図２８に示すフローチャートと異なるだけであり、他のステップについては図２８および図２９と同様であるので、ここでは説明を省略する。

【０１４７】

次に、図２８および図２９で示した蓄積コンテンツの視聴中において、コンテンツのタイムスキップを行う場合の動作を、図３０に示すフローチャートを用いて説明する。

ユーザが、端末アプリケーション２１１１を通じて、再生中のコンテンツのタイムスキップを要求すると、コンテンツ利用制御部２１０６は、スキップ先の位置を取得する（ステップＳ３００１）。具体的には、コンテンツ利用制御部２１０６は、ユーザにより指定されたスキップ先についての時刻情報（現在再生している箇所からの秒数など）を取得する。

【０１４８】

コンテンツ利用制御部２１０６は、現在の再生箇所のＰＴＳ１３４３ａ（以下、ＰＴＳ＿Ｓｒｃと記述）と、スキップ先のＰＴＳ１３４３ａ（以下、ＰＴＳ＿Ｄｓｔと記述）を取得する（ステップＳ３００２）。具体的には、コンテンツ利用制御部２１０６は、コンテンツ利用部２１０８から現在再生している箇所のＰＴＳ１３４３ａ（最近に表示したフレームに付与されていたＰＴＳ１３４３ａ）を取得するとともに、ステップＳ３００１で取得したスキップ先の時刻情報を、ＰＴＳ１３４３ａに基づく値に変換する。例えば、ステップＳ３００１で取得した時刻情報が現在再生している箇所からの秒数である場合には、ＰＴＳ＿Ｓｒｃに当該時刻情報をＰＴＳ１３４３ａのクロックである９００００で除した値を加算することにより、スキップ先のＰＴＳ１３４３ａであるＰＴＳ＿Ｄｓｔの値が得られる。なお、コンテンツ利用制御部２１０６がＰＴＳ＿Ｓｒｃの値を取得する方法の一例としては、外部からアクセス可能なコンテンツ利用部２１０８の内部レジスタに、現在再生している箇所のＰＴＳ１３４３ａの値を随時書き込む方法が挙げられる。

【０１４９】

コンテンツ利用制御部２１０６は、ライセンス処理部２１０４から取得した再生制御情報に基づき、タイムスキップ（特殊再生）の制御期間内であるかどうかを判定する（ステップＳ３００３）。具体的には、コンテンツ利用制御部２１０６は、再生制御情報（制御情報１５０３）の制御ＩＤ１５１１が「特殊再生不可」となっている情報を含む場合に、セキュアな計時部（図２１に図示せず）から取得した日時情報と制御期限１５１２の値とを比較することにより、現在が特殊再生を制御すべき期間であるかどうかを判定する。

【０１５０】

ステップＳ３００３において、ＹＥＳである場合、すなわち、現在が特殊再生を制御すべき期間である場合には、ステップＳ３００４を実行する。

ステップＳ３００３において、ＮＯである場合、すなわち、現在が特殊再生を制御すべき期間でない場合には、ステップＳ３００６を実行する。

コンテンツ利用制御部２１０６は、ライセンス処理部２１０４から取得した再生制御情報に基づき、タイムスキップ（特殊再生）を行える区間であるかどうかを判定する（ステップＳ３００４）。具体的には、コンテンツ利用制御部２１０６は、再生制御情報（制御情報１５０３）の制御ＩＤ１５１１が「特殊再生不可」となっている情報を含む場合に、制御範囲１５１４で指定されるＰＴＳ１３４３ａの範囲である制御開始時刻～制御終了時刻が、ＰＴＳ＿Ｓｒｃ～ＰＴＳ＿Ｄｓｔに含まれるかどうかを、制御時刻個数１５２０の分だけチェックする。すなわち、現在再生している箇所とスキップ先の箇所とで表される区間が、少なくとも１つのＣＭスキップ禁止区間の一部または全部（制御情報１５０３の制御開始時刻～制御終了時刻）を包含する場合を検出している。

【０１５１】

ステップＳ３００４において、ＹＥＳである場合、すなわち、ＰＴＳ＿Ｓｒｃ～ＰＴＳ＿ＤｓｔにＣＭスキップ禁止箇所が含まれる場合は、ステップＳ３００５を実行する。

ステップＳ３００４において、ＮＯである場合、すなわち、ＰＴＳ＿Ｓｒｃ～ＰＴＳ＿ＤｓｔにＣＭスキップ禁止箇所が含まれない場合は、ステップＳ３００６を実行する。

コンテンツ利用制御部２１０６は、当該コンテンツの視聴履歴を取得して、ＰＴＳ＿Ｓｒｃ～ＰＴＳ＿Ｄｓｔに含まれるＣＭスキップ禁止箇所の過去の視聴回数が、規定数以上であるかどうかを判定する（ステップＳ３００５）。具体的には、コンテンツ利用制御部２１０６は、視聴履歴ＤＢ２１０６を検索して、視聴履歴ＤＢ２１０６に蓄積されたＵＬ２２００の内、コンテンツＩＤ２２０５が一致するＵＬ２２００の視聴履歴である時刻情報２２１０を参照する。時刻情報２２１０は、当該コンテンツを過去に視聴したＰＴＳ１３４３ａの値が記載されているので、ＰＴＳ＿Ｓｒｃ～ＰＴＳ＿Ｄｓｔに含まれるＣＭスキップ禁止箇所が含まれている回数をカウントして、制御情報１５０３の制御回数１５１３と比較する処理を行う。

【０１５２】

ステップＳ３００５において、ＰＴＳ＿Ｓｒｃ～ＰＴＳ＿Ｄｓｔに含まれるＣＭスキップ禁止箇所の過去の視聴回数が、制御回数１５１３以上である場合には、ステップＳ３００６を実行する。

ステップＳ３００５において、ＰＴＳ＿Ｓｒｃ～ＰＴＳ＿Ｄｓｔに含まれるＣＭスキップ禁止箇所の過去の視聴回数が、制御回数１５１３未満である場合には、ステップＳ３００７を実行する。

【０１５３】

コンテンツ利用制御部２１０６は、タイムスキップを実行する（ステップＳ３００６）。具体的にはコンテンツ利用制御部２１０６は、指定されたスキップ先のＴＳパケット１４００をコンテンツ蓄積部２１０３から取得するよう、コンテンツ復号部２１０７およびコンテンツ利用部２１０８を制御する。スキップ後の処理の動作は、図２９で説明した動作と同様である。

【０１５４】

コンテンツ利用制御部２１０６は、タイムスキップ動作を禁止する（ステップＳ３００７）。具体的には、コンテンツ利用制御部２１０６は、タイムスキップ動作が不可である旨を（必要に応じてその理由とともに）、端末アプリケーション２１１１のユーザインタフェースを通じてユーザに通知する。

なお、ここではタイムスキップを行う場合の例を示したが、他の特殊再生の場合も同様の制御を行うことにより、ＣＭなどコンテンツの特定箇所の特殊再生を防止することが可能である。

【０１５５】

例えば、図３１は、図２８および図２９で示した蓄積コンテンツの視聴中において、コンテンツの早送りを行う場合の動作を示すフローチャートである。

図３１において、ユーザが端末アプリケーション２１１１を通じて再生中のコンテンツの早送りを要求すると、コンテンツ利用制御部２１０６は早送り指示を受信する（ステップＳ３１０１）。具体的には、コンテンツ利用制御部２１０６は、端末アプリケーション２１１１から早送りを示すアクションＩＤを受信する。

【０１５６】

コンテンツ利用制御部２１０６は、ライセンス処理部２１０４から取得した再生制御情報に基づき、早送り（特殊再生）の制御期間内であるかどうかを判定する（ステップＳ３１０２）。具体的には、コンテンツ利用制御部２１０６は、再生制御情報（制御情報１５０３）の制御ＩＤ１５１１が「特殊再生不可」となっている情報を含む場合に、セキュアな計時部（図２１に図示せず）から取得した日時情報と制御期限１５１２の値とを比較することにより、現在が特殊再生を制御すべき期間であるかどうかを判定する。

【０１５７】

ステップＳ３１０２において、ＹＥＳである場合、すなわち、現在が特殊再生を制御すべき期間である場合には、ステップＳ３１０３を実行する。

ステップＳ３１０２において、ＮＯである場合、すなわち、現在が特殊再生を制御すべき期間でない場合には、ステップＳ３１０６を実行する。

コンテンツ利用制御部２１０６は、現在の再生箇所のＰＴＳ１３４３ａ（以下、ＰＴＳ

＿Ｓｒｃと記述）を取得する（ステップＳ３１０３）。具体的には、コンテンツ利用制御部２１０６は、コンテンツ利用部２１０８から現在再生している箇所のＰＴＳ1343ａ（最近に表示したフレームに付与されていたＰＴＳ１３４３ａ）を取得する。

【０１５８】

コンテンツ利用制御部２１０６は、ライセンス処理部２１０４から取得した再生制御情報に基づき、早送り（特殊再生）を行える区間であるかどうかを判定する（ステップＳ３１０４）。具体的には、コンテンツ利用制御部２１０６は、再生制御情報（制御情報１５０３）の制御ＩＤ１５１１が「特殊再生不可」となっている情報を含む場合に、制御範囲１５１４で指定されるＰＴＳ１３４３ａの範囲である制御開始時刻～制御終了時刻に、ＰＴＳ＿Ｓｒｃが含まれるかどうかを制御時刻個数１５２０の分だけチェックする。すなわち、現在再生している箇所が、少なくとも１つのＣＭスキップ禁止区間に（制御情報１５０３の制御開始時刻～制御終了時刻）包含される場合を検出している。

【０１５９】

ステップＳ３１０４において、ＹＥＳである場合、すなわち、ＰＴＳ＿ＳｒｃがＣＭスキップ禁止箇所に含まれる場合は、ステップＳ３１０５を実行する。

ステップＳ３１０４において、ＮＯである場合、すなわち、ＰＴＳ＿ＳｒｃがＣＭスキップ禁止箇所に含まれない場合は、ステップＳ３１０６を実行する。

コンテンツ利用制御部２１０６は、当該コンテンツの視聴履歴を取得して、ＰＴＳ＿Ｓｒｃが含まれるＣＭスキップ禁止箇所の過去の視聴回数が、規定数以上であるかどうかを判定する（ステップＳ３１０５）。具体的には、コンテンツ利用制御部２１０６は、視聴履歴ＤＢ２１０６を検索して、視聴履歴ＤＢ２１０６に蓄積されたＵＬ２２００の内、コンテンツＩＤ２２０５が一致するＵＬ２２００の視聴履歴である時刻情報２２１０を参照する。時刻情報２２１０は、当該コンテンツを過去に視聴したＰＴＳ１３４３ａの値が記載されているので、ＰＴＳ＿Ｓｒｃが含まれるＣＭスキップ禁止箇所を視聴した履歴数をカウントして、制御情報１５０３の制御回数１５１３と比較する処理を行う。

【０１６０】

ステップＳ３１０５において、ＰＴＳ＿Ｓｒｃが含まれるＣＭスキップ禁止箇所の過去の視聴回数が、制御回数１５１３以上である場合には、ステップＳ３１０６を実行する。

ステップＳ３１０５において、ＰＴＳ＿Ｓｒｃが含まれるＣＭスキップ禁止箇所の過去の視聴回数が、制御回数１５１３未満である場合には、ステップＳ３１０７を実行する。

コンテンツ利用制御部２１０６は、早送りを実行する（ステップＳ３１０６）。具体的にはコンテンツ利用制御部２１０６は、早送りの速度に対応した分のＴＳパケット１４００をコンテンツ蓄積部２１０３から取得するよう、コンテンツ復号部２１０７およびコンテンツ利用部２１０８を制御する。通常、早送りではＭＰＥＧのＩピクチャのみを表示することが多いため、ＴＳパケット１４００のＴＳＰ　Ｈｅａｄｅｒ１４１０やＡｄａｐｔａｔｉｏｎ　Ｆｉｅｌｄ１４２０の情報を参照しながら、Ｉピクチャのみのパケット１４００を選択する処理を行う。スキップ後の処理の動作は、図２９で説明した動作と同様である。また、早送りにともなって変化する再生箇所が、ＣＭスキップ禁止箇所か否かを逐次判定するため、ステップＳ３１０２～ステップＳ３１０６の処理を繰り返し実行する。なお、ステップＳ３１０２～ステップＳ３１０６の処理を繰り返し実行する際には、必要に応じて、ステップＳ３１０５の処理は省略しても可である。この場合、ステップＳ３１０５における処理は全てＮＯとして処理され、ステップＳ３１０７が実行される。

【０１６１】

コンテンツ利用制御部２１０６は、早送り動作を禁止する（ステップＳ３１０７）。具体的には、コンテンツ利用制御部２１０６は、早送り動作が不可である旨を（必要に応じてその理由とともに）、端末アプリケーション２１１１のユーザインタフェースを通じてユーザに通知する。

このように、コンテンツの特定箇所に関して、期間限定かつ回数限定で該当部分の特殊再生を制御することができる。

【０１６２】

さらに、本発明における実施の形態で述べた制御方法は、特殊再生の場合に限らず、コンテンツの特定部分の視聴を制御するという目的にも利用できる。この場合の例として、ＰＰＶコンテンツのプレビュー部分の視聴を制御する動作を、図３２を用いて説明する。図３２では、図３０および図３１と同様、コンテンツの視聴中において、コンテンツのプレビューを行う場合の動作を示すフローチャートである。

【０１６３】

ユーザが端末アプリケーション２１１１を通じて、あるコンテンツのプレビュー再生を要求すると、コンテンツ利用制御部２１０６はプレビュー指示を受信する（ステップＳ３２０１）。具体的には、コンテンツ利用制御部２１０６は、端末アプリケーション２１１１からプレビューを示すアクションＩＤを受信する。

コンテンツ利用制御部２１０６は、ライセンス処理部２１０４から取得した再生制御情報に基づき、プレビューの制御期間内であるかどうかを判定する（ステップＳ３２０２）。具体的には、コンテンツ利用制御部２１０６は、再生制御情報（制御情報１５０３）の制御ＩＤ１５１１が「プレビュー可」となっている情報を含む場合に、セキュアな計時部（図２１に図示せず）から取得した日時情報と制御期限１５１２の値とを比較することにより、現在がプレビューを実行可能な期間であるかどうかを判定する。

【０１６４】

ステップＳ３２０２において、ＹＥＳである場合、すなわち、現在がプレビューを実行可能な期間である場合には、ステップＳ３２０３を実行する。

ステップＳ３２０２において、ＮＯである場合、すなわち、現在がプレビューを実行可能な期間でない場合には、ステップＳ３２０７を実行する。

コンテンツ利用制御部２１０６は、現在の再生箇所のＰＴＳ１３４３ａ（以下、ＰＴＳ＿Ｓｒｃと記述）を取得する（ステップＳ３２０３）。具体的には、コンテンツ利用制御部２１０６は、コンテンツ利用部２１０８から現在再生している箇所のＰＴＳ１３４３ａ（最近に表示したフレームに付与されていたＰＴＳ１３４３ａ）を取得する。

【０１６５】

コンテンツ利用制御部２１０６は、ライセンス処理部２１０４から取得した再生制御情報に基づき、プレビューが可能な区間であるかどうかを判定する（ステップＳ３２０４）。具体的には、コンテンツ利用制御部２１０６は、再生制御情報（制御情報１５０３）の制御ＩＤ１５１１が「プレビュー可」となっている情報を含む場合に、制御範囲１５１４で指定されるＰＴＳ１３４３ａの範囲である制御開始時刻～制御終了時刻に、ＰＴＳ＿Ｓｒｃが含まれるかどうかを制御時刻個数１５２０の分だけチェックする。すなわち、現在再生している箇所が、少なくとも１つのプレビュー可能区間に（制御情報１５０３の制御開始時刻～制御終了時刻）包含される場合を検出している。

【０１６６】

ステップＳ３２０４において、ＹＥＳである場合、すなわち、ＰＴＳ＿Ｓｒｃがプレビュー可能区間に含まれる場合は、ステップＳ３２０５を実行する。

ステップＳ３２０４において、ＮＯである場合、すなわち、ＰＴＳ＿Ｓｒｃがプレビュー可能区間に含まれない場合は、ステップＳ３２０７を実行する。

コンテンツ利用制御部２１０６は、当該コンテンツの視聴履歴を取得して、ＰＴＳ＿Ｓｒｃが含まれるプレビュー可能箇所の過去の視聴回数が、規定数以上であるかどうかを判定する（ステップＳ３２０５）。具体的には、コンテンツ利用制御部２１０６は、視聴履歴ＤＢ２１０６を検索して、視聴履歴ＤＢ２１０６に蓄積されたＵＬ２２００の内、コンテンツＩＤ２２０５が一致するＵＬ２２００の視聴履歴である時刻情報２２１０を参照する。時刻情報２２１０は、当該コンテンツを過去に視聴したＰＴＳ１３４３ａの値が記載されているので、ＰＴＳ＿Ｓｒｃが含まれるプレビュー可能箇所を視聴した履歴数をカウントして、制御情報１５０３の制御回数１５１３と比較する処理を行う。

【０１６７】

ステップＳ３２０５において、ＰＴＳ＿Ｓｒｃが含まれるプレビュー可能箇所の過去の視聴回数が、制御回数１５１３以上である場合には、ステップＳ３２０７を実行する。

ステップＳ３２０５において、ＰＴＳ＿Ｓｒｃが含まれるプレビュー可能箇所の過去の視聴回数が、制御回数１５１３未満である場合には、ステップＳ３２０６を実行する。

コンテンツ利用制御部２１０６は、プレビューを実行する（ステップＳ３２０６）。具体的にはコンテンツ利用制御部２１０６は、コンテンツのプレビューを許可し、コンテンツの復号およびコンテンツのデコードを実行する。また、プレビューにともなって再生箇所が変わっていくため、現在の再生箇所がプレビュー可能か否かを逐次判定するため、ステップＳ３２０２～ステップＳ３２０６の処理を繰り返し実行する。なお、ステップＳ３２０２～ステップＳ３２０６の処理を繰り返し実行する際には、必要に応じて、ステップＳ３２０５の処理は省略しても可である。この場合、ステップＳ３２０５における処理は全てＹＥＳとして処理され、ステップＳ３２０６が実行される。

【０１６８】

コンテンツ利用制御部２１０６は、プレビューを禁止する（ステップＳ３２０７）。具体的には、コンテンツ利用制御部２１０６は、プレビューが不可である旨を（必要に応じてその理由とともに）、端末アプリケーション２１１１のユーザインタフェースを通じてユーザに通知する。

このように、ＰＰＶコンテンツのプレビューに関して、期間限定かつ回数限定でプレビューを制御することができる。

【０１６９】

以上のように、コンテンツ利用制御システム１では、配信センター１０１が、コンテンツに付加した既存のセキュアな時刻情報を用いて、コンテンツの特定部分の利用を制御するための再生制御情報をコンテンツとは別データとしてセキュアに端末装置に配信するようにし、端末装置では、コンテンツに既存のセキュアな時刻情報と、配信センター１０１から取得した再生制御情報とを用いて、コンテンツの利用をセキュアに制御するようにしている。そのため、事業者は、既存のエンコーダを活用することができ、送出設備に関するコストを軽減できるとともに、事業者が、ユーザによるコンテンツの特定部分の利用をセキュアに制御することが可能となる。

【０１７０】

なお、本発明における実施の形態では、コンテンツに付加された時刻情報としてＰＥＳパケットのＰＴＳ１４４３ａを用いる場合の例を示したが、これに限られるものではなく、ＰＥＳパケットのＤＴＳ１４４３ｂ、ＴＳパケット１４００のＰＣＲ１４２５ａ、ＭＰＥＧ－４　ＳｙｓｔｅｍｓのＳＬ（Ｓｙｎｃ　Ｌａｙｅｒ）、ＭＰＥＧ－２　ＥＳのＧｒｏｕｐ　Ｏｆ　ＰｉｃｔｕｒｅのＴｉｍｅ　Ｃｏｄｅなど、コンテンツに既存の情報であり、かつ、コンテンツの部分を特定可能な情報を用いることが可能である。この場合、ＴＳパケット１４００のＰＣＲ１４２５ａなど暗号化されない時刻情報を用いる場合は、時刻情報の値をコンテンツの暗号鍵に関連させるか、時刻情報の値を含むデータに対するハッシュ値を付加するなど、時刻情報をセキュアに配信するための処理が必要となる。

【０１７１】

また、本発明における実施の形態では、ＭＰＥＧ－２　ＰＥＳ／ＴＳで多重化されたコンテンツの例を示したが、ＭＰＥＧ－２　ＰＳ（Ｐｒｏｇｒａｍ　Ｓｔｒｅａｍ）やＭＰＥＧ以外のコンテンツであっても、コンテンツに既存の情報であり、かつ、コンテンツの部分を特定可能な情報があれば適用することが可能であることは言うまでもない。

また、本発明における実施の形態では、ＡＲＩＢ　ＳＴＤ－Ｂ２５　４．１版に示されているサーバ型放送方式タイプＩに基づいてコンテンツを配信する場合の例を示したが、ファイル型コンテンツの配信方式であるサーバ型放送方式タイプIIの場合や、インターネット上でのストリーミング配信、ダウンロード配信などに適用可能であることは言うまでもない。この場合、一般的には、コンテンツは単一の暗号鍵Ｋｃ´で暗号化されるので、ライセンス（本発明における実施の形態におけるメインライセンス９００に相当）に暗号鍵Ｋｃ´を設定し、ライセンスを権利管理サーバ１０１ａからインターネットなどの通信経由で端末装置１０２に配信する。同様に、再生制御情報も、このライセンスに含める。このようにすることにより、コンテンツが時変鍵でスクランブルされておらず、単一の暗

号鍵で暗号化されている場合（すなわち、メインライセンス９００とサブライセンス１０００というライセンス構成ではなく、単一のライセンス構成の場合）においても、端末装置１０２でのコンテンツの特定部分の利用制御をセキュアに行うことができる。

【０１７２】

また、本発明における実施の形態では、視聴履歴であるＵＬ２２００において、ユーザＩＤ２１０３や端末ＩＤ２１０４をはじめとする種々の情報を記録するようにしたが、視聴履歴に基づくコンテンツ利用制御に用いるためには、コンテンツとコンテンツの視聴箇所を特定することができれば良いため、コンテンツＩＤ２１０５またはライセンスＩＤ２１０６、あるいはコンテンツＩＤ２１０５かつライセンスＩＤ２１０６（コンテンツ利用制御システム１内におけるＩＤの割り当てかたに依存する）と、１以上の開始時刻情報と終了時刻情報の組を記録すれば良い。

【０１７３】

また、本発明における実施の形態では、端末装置１０２において記録した視聴履歴を、視聴履歴ＤＢ２１１０で管理する場合の例を示したが、ライセンスＤＢ２１０５において管理されるライセンス（メインライセンス９００）とともに管理するようにしても良い。

また、本発明における実施の形態では、コンテンツの特定箇所の利用制御を行う場合の例としてＣＭスキップ制御を行う場合の例を示したが、これに限られるものではなく、例えば、ダイジェスト視聴のような、コンテンツの特定箇所だけを利用させるような制御にも適用できる。

【０１７４】

また、本発明における実施の形態では、再生制御情報における再生制御箇所の情報（制御情報１５４５）として、コンテンツに付与されたＰＴＳ１３４３ａの値そのものを用いて指定する場合の例を示したが、コンテンツの先頭でのＰＴＳ１３４３ａの値と、ＰＴＳ１３４３ａに基づくコンテンツの先頭からの相対値とを用いて、制御情報１５４５を構成するようにしても良い。また、制御情報１５４５において、再生制御箇所を制御開始時刻と制御終了時刻とで指定された範囲で表現したが、制御開始時刻と制御時間（時間幅）という表現にしても良い。

【０１７５】

また、本発明における実施の形態では、再生制御情報における再生制御箇所の情報（制御情報１５４５）として、特殊再生禁止区間（通常再生のみを許可する区間）を記述する場合の例を示したが、制御情報１５４５に特殊再生許可区間を記述するようにしても良い。

また、本発明における実施の形態では、再生制御情報をライセンス（サブライセンス１０００）、ＥＣＭに設定して、配信センター１０１から端末装置１０２に配信する場合の例を示したが、これに限られるものではなく、通信でＳＳＬなどのセキュアなチャネルを用いて配信したり、放送でのＥＭＭで配信したりするようにしても良い。よって本方式は、コンテンツへのＥＣＭなどの関連情報の多重化有無にかかわらず、統一的に適用可能な方式である。なお、このような場合、コンテンツ利用時点で端末装置１０２が再生制御情報（制御情報１５４５）を取得していない場合には、当該コンテンツの視聴においては通常再生しか許可しない、または、プレビューを許可しないように制御し、再生制御情報を取得後に特殊再生やプレビューなどを許可するように制御しても良い。

【０１７６】

また、コンテンツの先頭でのＰＴＳ１３４３ａの値と、ＰＴＳ１３４３ａに基づくコンテンツの先頭からの相対値とを用いて制御情報１５４５が構成される場合、コンテンツ配信サーバ１０１ｂにおけるストリーミングコンテンツの送出時にＰＴＳ１３４３ａに基づくコンテンツの先頭からの相対値で再生制御箇所を指定しておき、コンテンツの先頭のＰＴＳ１３４３ａが確定した後に、コンテンツの先頭のＰＴＳ１３４３ａをコンテンツ配信サーバ１０１ｂから端末装置１０２に配信するようにしても良い。このとき、端末装置１０２がコンテンツの先頭のＰＴＳ１３４３ａを取得していない間は、通常再生しか許可しない、または、プレビューを許可しないように制御する。

【０１７７】
また、本発明における実施の形態では、ライセンス（サブライセンス１０００）をＫｃ配信用ＥＣＭ１９００に設定して、配信センター１０１から端末装置１０２に配信する場合の例を示したが、これに限られるものではなく、ＥＣＭ－Ｋｗ１８００、ＥＣＭ－Ｋｃ１８１０や、ＥＭＭ（サーバ型放送方式タイプＩでのＫｃ配信用ＥＭＭも含む）で配信するようにしても良い。また、放送による配信では、ＥＣＭ－Ｋｗ１８００、ＥＣＭ－Ｋｃ１８１０を用い（必要に応じて、ワーク鍵Ｋｗ２０３の配信のためのＥＭＭを用いても良い）、コンテンツ鍵Ｋｃ２０５および再生制御情報を含むライセンスを、通信経由で配信するようにしても良い。

【０１７８】
また、本発明における実施の形態では、コンテンツの特定箇所の利用を制御する制御情報の例として、再生制御のための情報（再生制御情報）を配信する場合の例を示したが、これに限られるものではなく、印刷や編集など、端末装置１０２における再生以外の利用制御についても適用可能である。
また、本発明における実施の形態では、コンテンツ配信サーバ１０１ｂにおいて再生制御情報を生成する場合の例を示したが、権利管理サーバ１０１ａで生成するようにしても良い。この場合、コンテンツに付与されるＰＴＳ１３４３ａの情報をコンテンツ配信サーバ１０１ｂから権利管理サーバ１０１ａに通知する必要があることは言うまでもない。また、コンテンツ配信サーバ１０１ｂにおいて、サブライセンス１０００に再生制御情報を設定するようにしたが、権利管理サーバ１０１ｂで設定するようにしても良い。

【０１７９】
また、本発明における実施の形態では、端末装置１０２において、全てのコンテンツ利用に対する視聴履歴を記録する場合の例を示したが、メインライセンス９００あるいはサブライセンス１０００に視聴履歴の記録を指示する情報を含めておくことにより、これに従ってコンテンツ毎やライセンス毎、あるいは、ユーザ毎に視聴履歴を記録するかどうかの制御を行うようにしても良い。

【０１８０】
また、本発明における実施の形態では、コンテンツ配信サーバ１０１ｂにおける再生制御情報生成部１１０６が、再生制御情報の生成にあたりコンテンツ符号化部１１０５からＰＴＳ１３４３ａの値を取得する場合の例を示したが、時刻情報付加部１１０４からＳＴＣの値を直接取得するようにしても良い。但し、この場合、コンテンツ符号化部１１０５が用いるＳＴＣの値と、再生制御情報生成部１１０６が用いるＳＴＣの値は一致する必要があることは言うまでもない。

【０１８１】
また、本発明における実施の形態では、コンテンツ配信サーバ１０１ｂにおける再生制御情報生成部１１０６が、ストリーミングコンテンツ（リアルタイムエンコード）する場合において、コンテンツの先頭のＰＴＳ１３４３ａの値を算出して、再生制御情報を生成する場合の例を示したが、ダウンロードコンテンツ（プリエンコード）する場合においては、予めコンテンツのコンテンツ先頭のＰＴＳ１３４３ａの値や、ＣＭ箇所、プレビュー可能箇所などのＰＴＳ１３４３ａの値を特定することができるため、実際にコンテンツに付加されたＰＴＳ１３４３ａの値に基づき、再生制御情報を生成することが可能である。

【０１８２】
また、本発明における実施の形態では、再生制御情報（制御情報１５０３）の制御ＩＤ１５１１として、「特殊再生不可」、「プレビュー可」というＩＤを用いる場合の例を示したが、端末装置１０２におけるユーザの操作やコンテンツの処理を規定するための識別子であれば、これに限られるものではない。
また、本発明における実施の形態では、制御ＩＤ１５１１に対して視聴履歴に基づく過去の視聴回数や、絶対時刻により制御期限などの制約が加えられている場合の例を示したが、過去の視聴時間などの制約を加えるようにしても良い。

【０１８３】

また、本発明における実施の形態では、視聴履歴ＤＢ２１１０に蓄積された視聴履歴を用いて、コンテンツの特定箇所の再生制御を行う場合の例を示したが、視聴履歴に基づき再生制御情報（制御情報１５４５）を変更するようにしても良い。例えば、特殊再生禁止区間を規定回数以上視聴した場合は、制御情報１５４５から該当の特殊再生禁止区間の情報を削除する。これにより、視聴履歴を配信センター１０１などに送信した後であっても、視聴履歴に基づく再生制御が可能となる。

【０１８４】

また、本発明における実施の形態では、再生制御情報をＫｃ配信用ＥＣＭ１９００に設定する場合の例を示したが、ＥＣＭ－Ｋｗ１８００やＥＣＭ－Ｋｃ１８１０に設定するようにしても良い。このとき、ＥＣＭ－Ｋｗ１８００とＥＣＭ－Ｋｃ１８１０、または、ＥＣＭ－Ｋｗ１８００とＫｃ配信用ＥＣＭ１９００に異なる再生制御情報を設定するようにすれば、リアルタイム視聴時と蓄積視聴時で異なる再生制御範囲が実現できる。例えば、プレビューの場合は、リアルタイム視聴時は先頭から一定時間といった画一的なプレビュー区間とならざるを得ないが、蓄積視聴時はダイジェスト視聴のようなコンテンツの特徴を生かしたプレビュー範囲を設定することができ、端末機能１０２の蓄積機能を十分に生かしたサービス提供が可能となる。

【０１８５】

さらに、本発明における実施の形態では、単一の配信経路からコンテンツやライセンス、制御情報などを取得する場合の例を示したが、デジタル放送とインターネットを併用したり、パッケージメディアとインターネットを併用したりといった、複合的な配信経路から取り込むようにすることもできる。

【産業上の利用可能性】

【０１８６】

本発明にかかるコンテンツ利用制御システムは、コンテンツに制御情報を追加することなく、コンテンツに既存のセキュアな時刻情報を用いて、端末装置でのコンテンツのＣＭ部分などのコンテンツの特定部分の利用制御をセキュアに実現することにより、低廉なコストで事業者の意図に反するユーザのコンテンツ利用を防止できるという効果を有し、デジタル放送、ＣＡＴＶ、インターネットなどによるコンテンツ配信サービスにおけるコンテンツ利用制御システムなどとして有用である。またパッケージメディアなどの可搬メディアなどによるコンテンツ配信サービスにおけるコンテンツ利用制御システムにも応用できる。

【図面の簡単な説明】

【０１８７】

【図１】本発明の実施の形態に係るコンテンツ利用制御システム１の全体の概略構成を示す図

【図２】本発明の実施の形態に係る暗号鍵スキームの概要を示す図

【図３】本発明の実施の形態に係る権利管理サーバ１０１ａの構成を示す機能ブロック図

【図４】本発明の実施の形態に係る鍵情報ＤＢ３０１のワーク鍵管理テーブルの構成を示す図

【図５】本発明の実施の形態に係る鍵情報ＤＢ３０１のコンテンツ鍵管理テーブルの構成を示す図

【図６】本発明の実施の形態に係るユーザ情報ＤＢ３０２のテーブル構成を示す図

【図７】本発明の実施の形態に係る利用条件ＤＢ３０３のテーブル構成を示す図

【図８】本発明の実施の形態に係るコンテンツ情報ＤＢ３０４のテーブル構成を示す図

【図９】本発明の実施の形態に係るメインライセンス９００の構成を示す図

【図１０】本発明の実施の形態に係るサブライセンス１０００の構成を示す図

【図１１】本発明の実施の形態に係るコンテンツ配信サーバ１０１ｂの構成を示す機能ブロック図

【図１２】本発明の実施の形態に係るコンテンツ属性情報ＤＢ１１０２のテーブル構成を示す図
【図１３】本発明の実施の形態に係るＰＥＳパケット１３００の概略構成を示す図
【図１４】本発明の実施の形態に係るＴＳパケット１４００の概略構成を示す図
【図１５】本発明の実施の形態に係る制御情報タグブロック１５００の構成を示す図
【図１６】本発明の実施の形態に係るコンテンツ送出開始時のＰＴＳ１３４３ａを算出する方法の概略を示す図
【図１７】本発明の実施の形態に係る制御情報１５０３の一例を示す図
【図１８】本発明の実施の形態に係るＥＣＭ－Ｋｗ１８００、ＥＣＭ－Ｋｃ１８１０の構成を示す図
【図１９】本発明の実施の形態に係るＫｃ配布用ＥＣＭ１９００の構成を示す図
【図２０】本発明の実施の形態に係る制御情報タグブロック１５００挿入後のサブライセンス１０００の構成を示す図
【図２１】本発明の実施の形態に係る端末装置１０２の構成を示す図
【図２２】本発明の実施の形態に係るＵＬ２２００の構成を示す図
【図２３】本発明の実施の形態に係るＥＬＩ２３００の構成を示す図
【図２４】本発明の実施の形態に係る端末装置１０２における権利管理サーバ１０１ａからのメインライセンス９００の取得処理を示すフローチャート
【図２５】本発明の実施の形態に係る権利管理サーバ１０１ａにおけるライセンス発行可否判定処理を示すフローチャート
【図２６】本発明の実施の形態に係る権利管理サーバ１０１ａにおけるサブライセンス１０００を生成する処理、および、ワーク鍵Ｋｗ２０３、コンテンツ鍵Ｋｃ２０５、サブライセンス１０００を送信する処理を示すフローチャート
【図２７】本発明の実施の形態に係るコンテンツ配信サーバ１０１ｂにおけるＥＣＭ生成処理、および、コンテンツ送出処理を示すフローチャート
【図２８】本発明の実施の形態に係る端末装置１０２におけるコンテンツ利用処理、および、ライセンス利用判定処理を示すフローチャート
【図２９】本発明の実施の形態に係る端末装置１０２におけるコンテンツ利用処理を示すフローチャート
【図３０】本発明の実施の形態に係る端末装置１０２におけるＣＭ部分のタイムスキップ制御処理を示すフローチャート
【図３１】本発明の実施の形態に係る端末装置１０２におけるＣＭ部分の早送り制御処理を示すフローチャート
【図３２】本発明の実施の形態に係る端末装置１０２におけるプレビュー制御処理を示すフローチャート

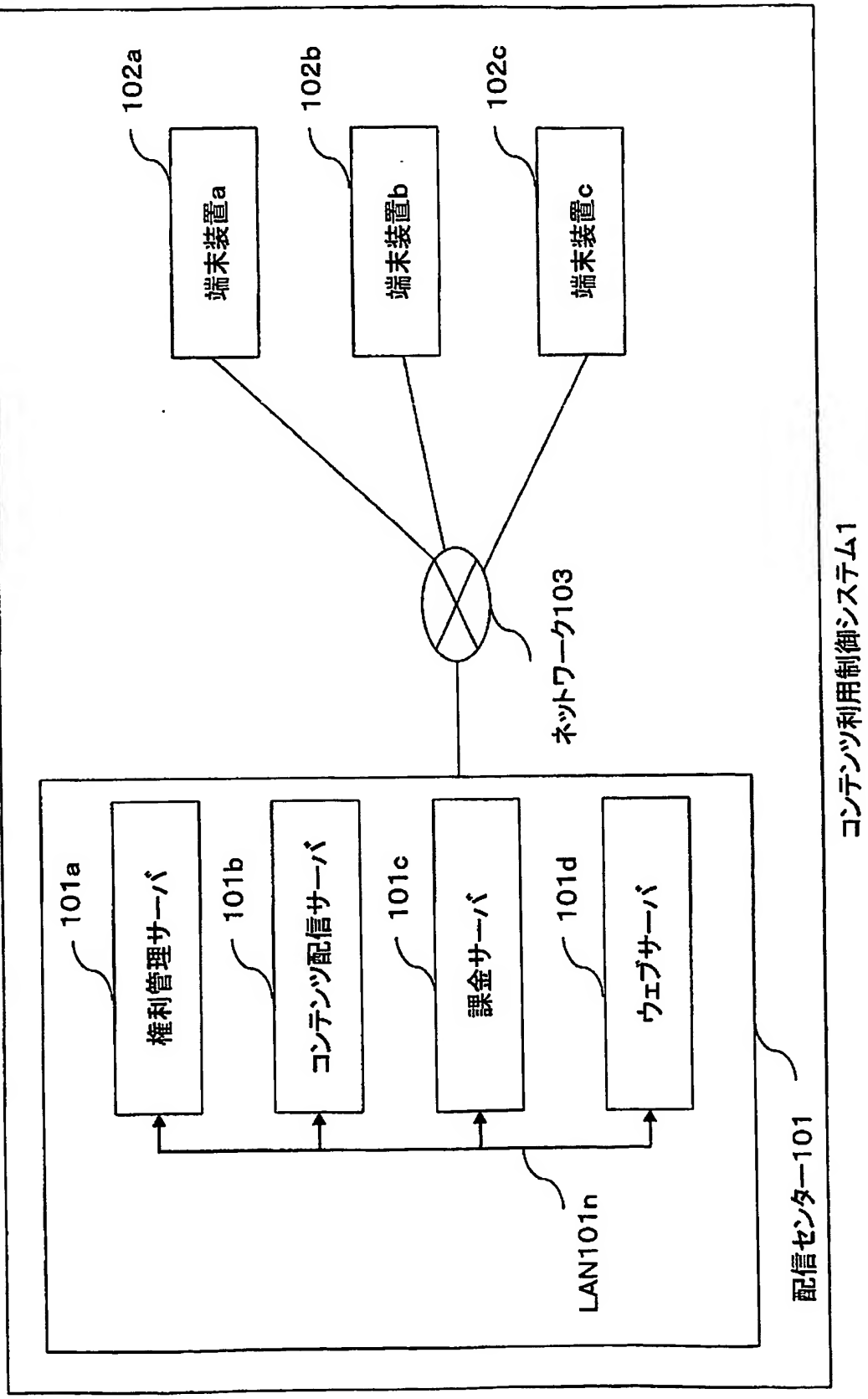
【符号の説明】

【０１８８】

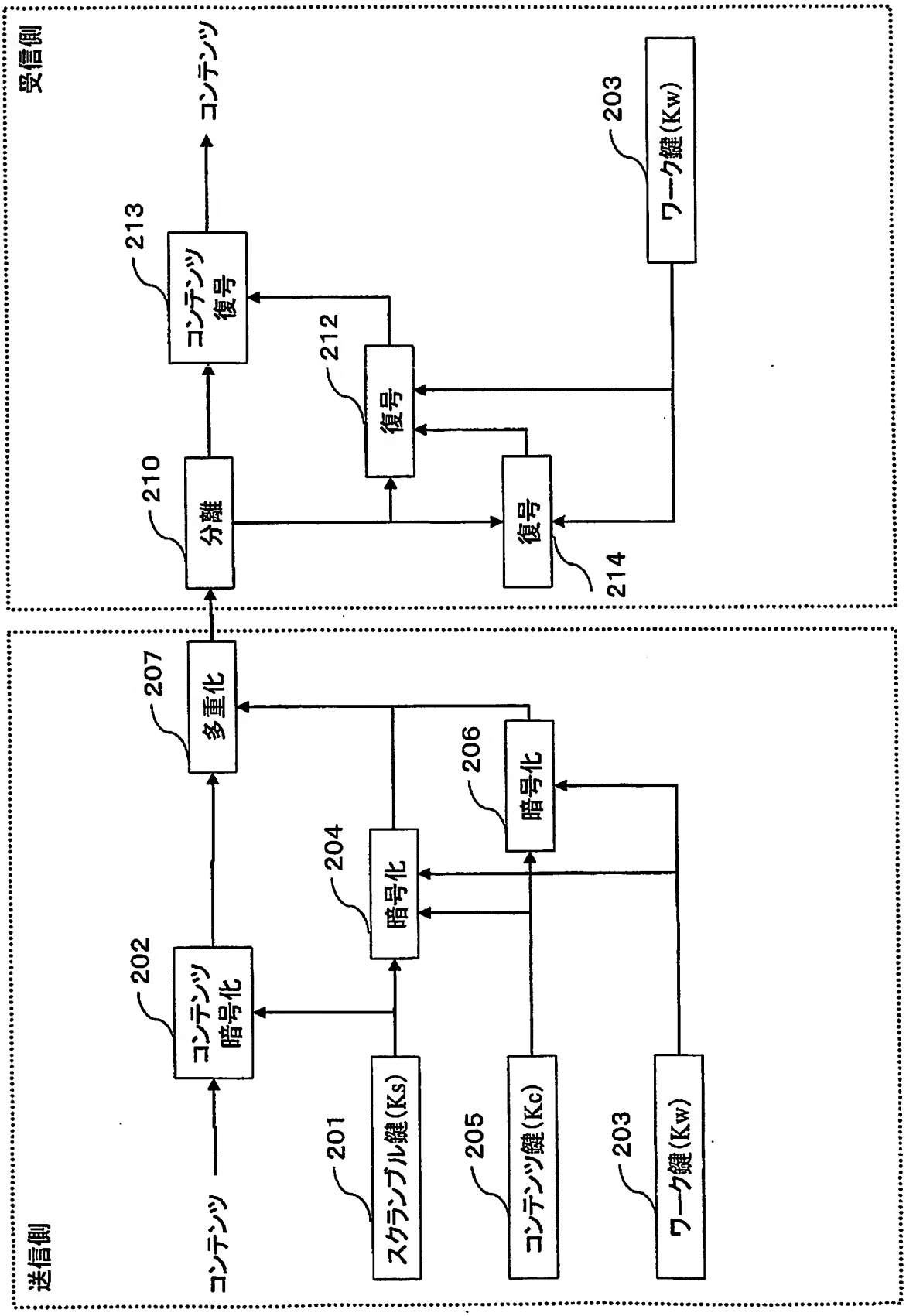
１　コンテンツ利用制御システム
１０１　配信センター
１０１ａ　権利管理サーバ
１０１ｂ　コンテンツ配信サーバ
１０１ｃ　課金サーバ
１０１ｄ　ウェブサーバ
１０１ｎ　ＬＡＮ
１０２　端末装置
１０３　ネットワーク
２０１　スクランブル鍵Ｋｓ
２０５　コンテンツ鍵Ｋｃ
２０３　ワーク鍵Ｋｗ
３０１　鍵情報ＤＢ

３０２　ユーザ情報ＤＢ
３０３　利用条件ＤＢ
３０４　コンテンツ情報ＤＢ
３１１　ライセンス発行部
３１２　サーバ送受信部
１１０１　コンテンツＤＢ
１１０２　コンテンツ属性情報ＤＢ
１１０３　計時部
１１０４　時刻情報付加部
１１０５　コンテンツ符号化部
１１０６　再生制御情報生成部
１１０７　ＥＣＭ生成部
１１０８　コンテンツ多重化部
１１０９　コンテンツ暗号化部
１１１０　コンテンツ送出部
２１０１　端末送受信部
２１０２　分離部
２１０３　コンテンツ蓄積部
２１０４　ライセンス処理部
２１０５　ライセンスＤＢ
２１０６　コンテンツ利用制御部
２１０７　コンテンツ復号部
２１０８　コンテンツ利用部
２１０９　視聴履歴記録部
２１１０　視聴履歴ＤＢ

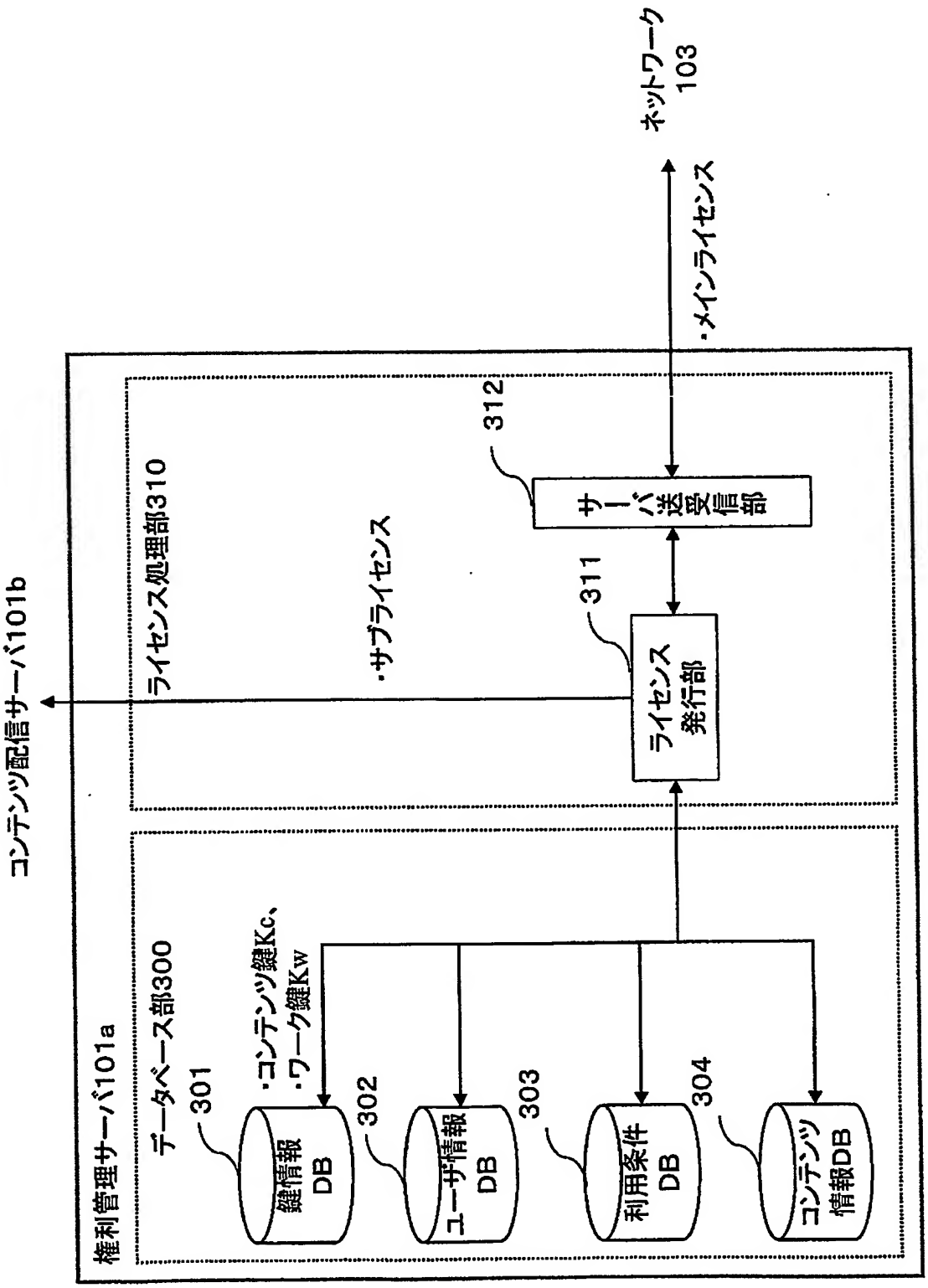
【書類名】図面
【図１】


102a
102b
102c
端末装置a
端末装置b
端末装置c
ネットワーク103
コンテンツ利用制御システム1
101a
101b
101c
101d
権利管理サーバ
コンテンツ配信サーバ
課金サーバ
ウェブサーバ
LAN101n
配信センター101

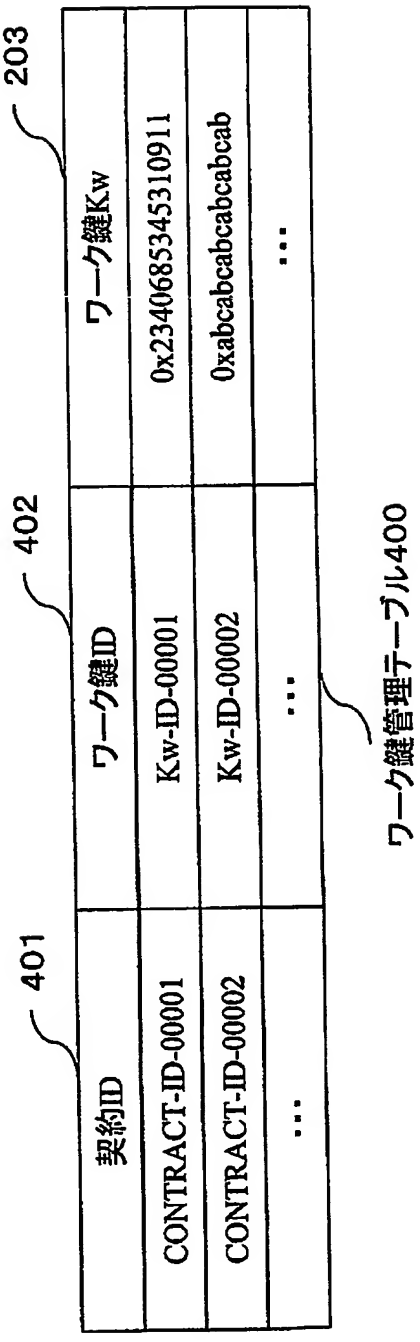
【図２】


送信側
コンテンツ
コンテンツ暗号化
202
スクランブル鍵(Ks)
201
暗号化
204
コンテンツ鍵(Kc)
205
暗号化
206
ワーク鍵(Kw)
203
多重化
207
分離
210
復号
212
復号
214
コンテンツ復号
213
コンテンツ
ワーク鍵(Kw)
203
受信側

【図３】


ネットワーク
103
・メインライセンス
312
サーバ送受信部
311
ライセンス
発行部
・サブライセンス
ライセンス処理部310
コンテンツ配信サーバ101b
権利管理サーバ101a
データベース部300
301
・コンテンツ鍵Kc、
・ワーク鍵Kw
鍵情報
DB
302
ユーザ情報
DB
303
利用条件
DB
304
コンテンツ
情報DB

【図４】


401
402
203
契約ID
ワーク鍵ID
ワーク鍵Kw
CONTRACT-ID-00001
Kw-ID-00001
0x2340685345310911
CONTRACT-ID-00002
Kw-ID-00002
0xabcabcabcabcabcab
…
…
…
ワーク鍵管理テーブル400

【図５】

501　　205

コンテンツID	コンテンツ鍵Kc
CONTENT-ID-00001	0x1234567890abcdef
CONTENT-ID-00002	0x43195745a4098b4e
CONTENT-ID-00003	0x3970584ad3922247
CONTENT-ID-00004	0x2411197120121974
・・・	・・・

コンテンツ鍵管理テーブル500

【図６】

601　　602

ユーザID	端末ID
USER-ID-00001	TERMINAL-ID-00001
USER-ID-00002	TERMINAL-ID-12345 TERMINAL-ID-54321
USER-ID-00003	TERMINAL-ID-77777
USER-ID-00004	TERMINAL-ID-99999
・・・	・・・

ユーザ情報管理テーブル600

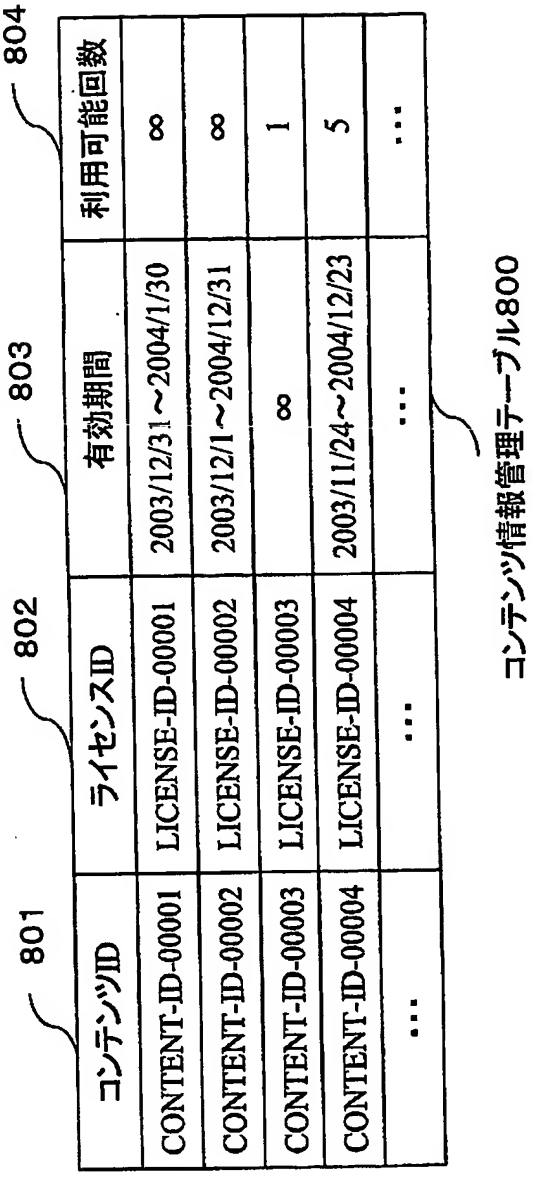
【図７】

ユーザID	利用条件ID	契約ID	有効期間	発行可能残回数
USER-ID-00001	URUs-ID-00001	CONTRACT-ID-00001	2002/12/31～2003/1/30	1
USER-ID-00002	URUs-ID-00002	CONTRACT-ID-13452	2002/12/1～2002/12/31	1
USER-ID-00002	URUs-ID-10011	CONTRACT-ID-99999	∞	3
USER-ID-00003	URUs-ID-24024	CONTRACT-ID-02804	2002/11/24～2002/12/23	2
...	...	...	...	...

701　702　703　704　705

利用条件管理テーブル700

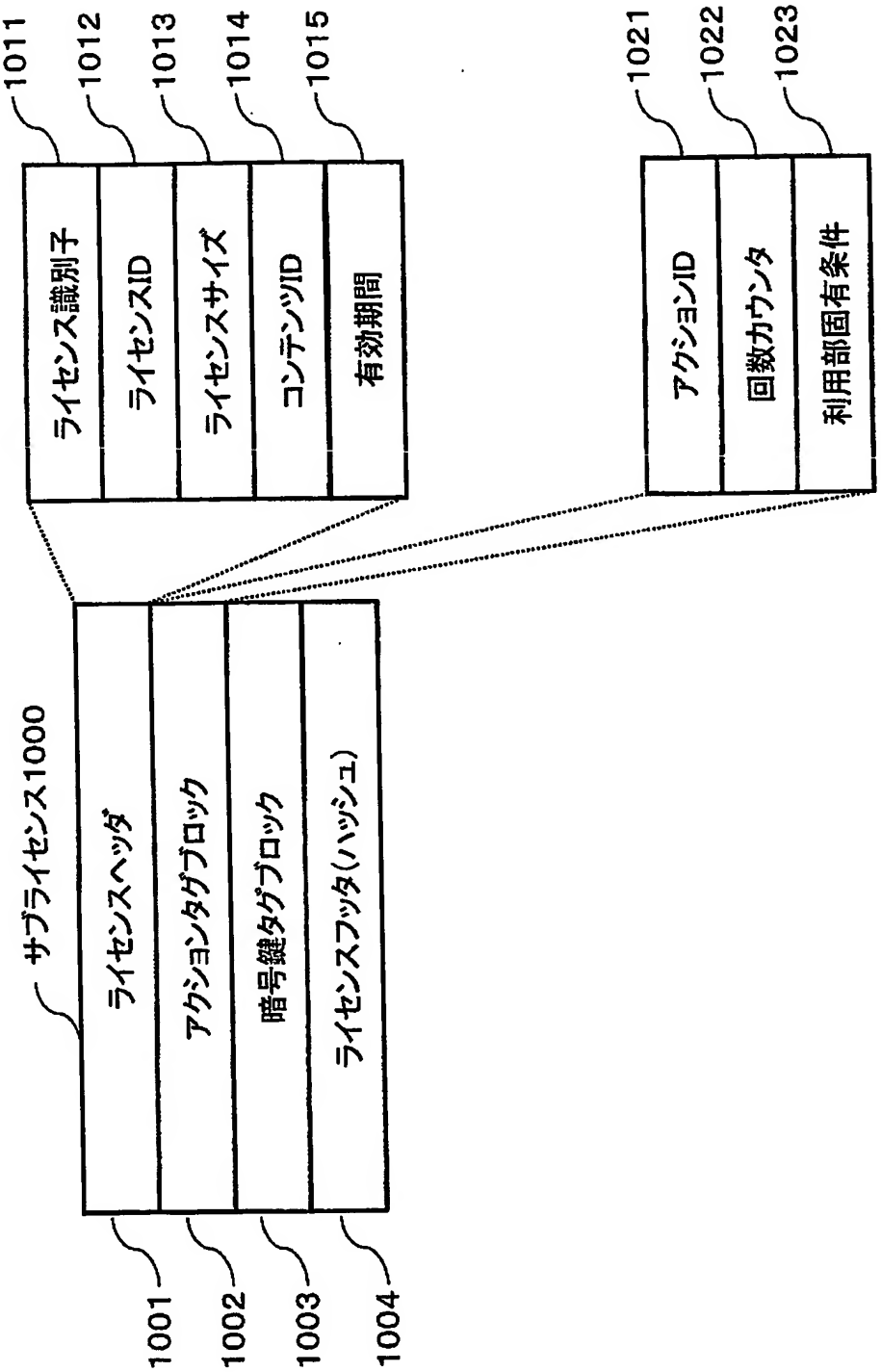
【図８】



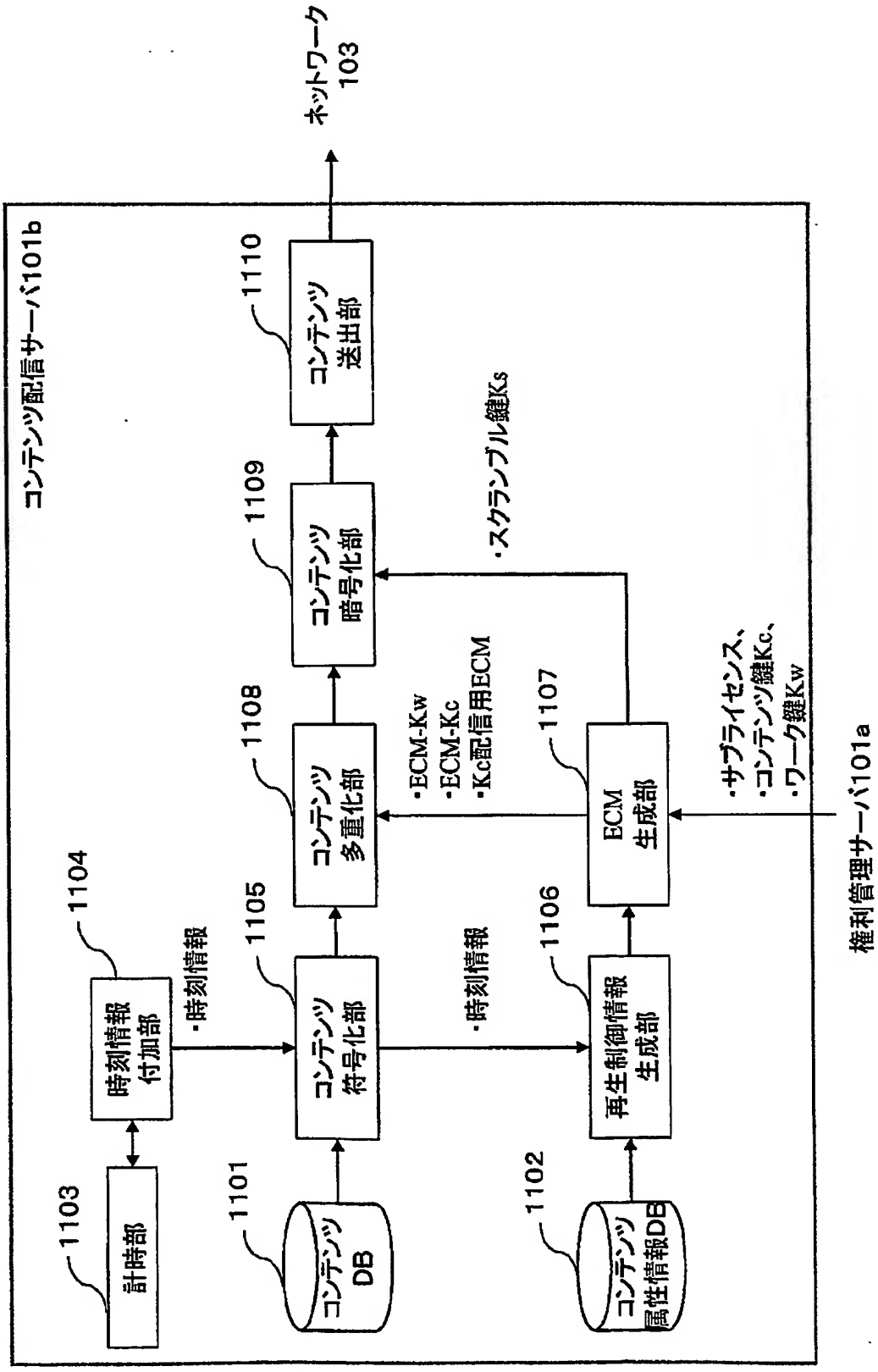
801 コンテンツID	802 ライセンスID	803 有効期間	804 利用可能回数
CONTENT-ID-00001	LICENSE-ID-00001	2003/12/31～2004/1/30	∞
CONTENT-ID-00002	LICENSE-ID-00002	2003/12/1～2004/12/31	∞
CONTENT-ID-00003	LICENSE-ID-00003	∞	1
CONTENT-ID-00004	LICENSE-ID-00004	2003/11/24～2004/12/23	5
…	…	…	…

コンテンツ情報管理テーブル800

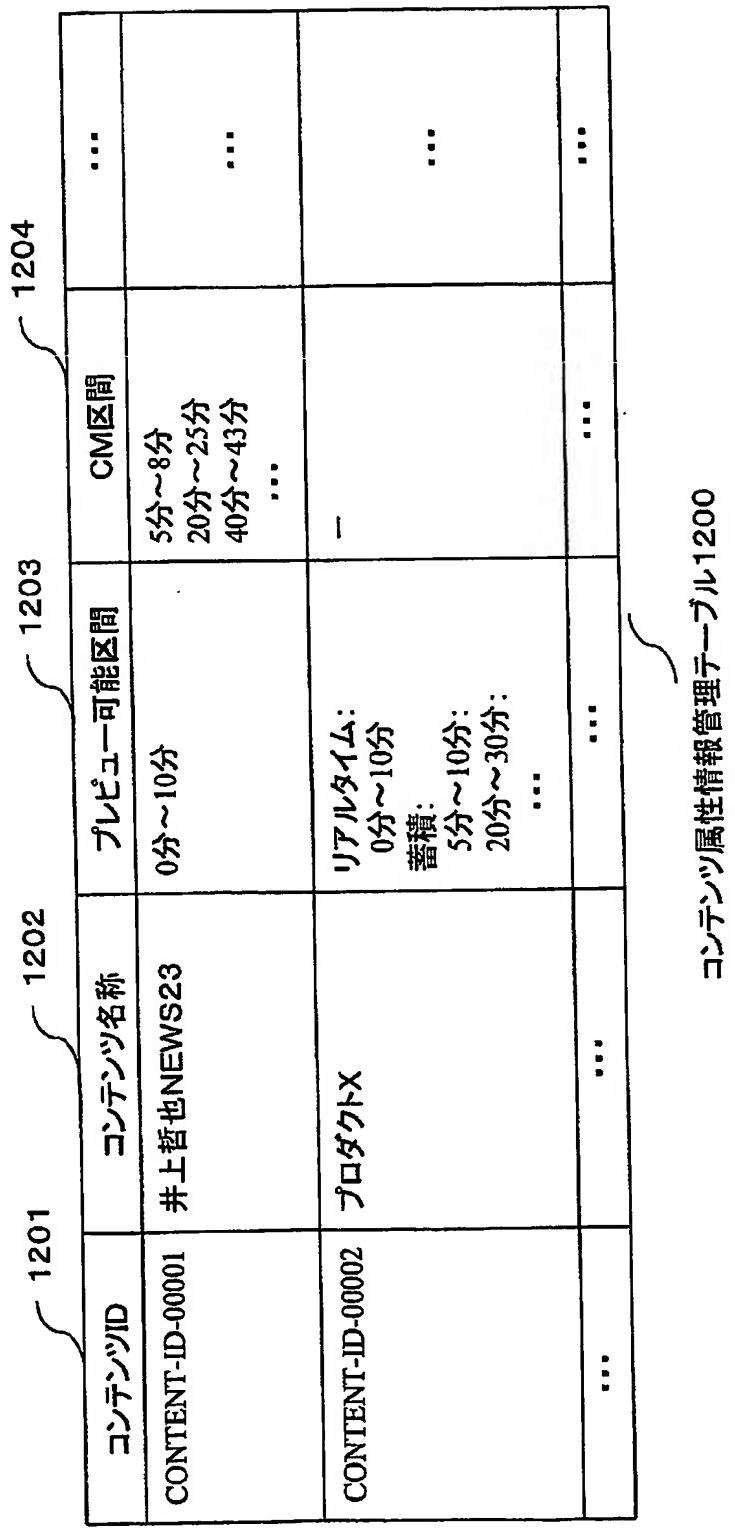
【図１０】


サブライセンス1000
ライセンスヘッダ
アクションタグブロック
暗号鍵タグブロック
ライセンスフッタ(ハッシュ)
1001
1002
1003
1004
ライセンス識別子
ライセンスID
ライセンスサイズ
コンテンツID
有効期間
1011
1012
1013
1014
1015
アクションID
回数カウンタ
利用部固有条件
1021
1022
1023

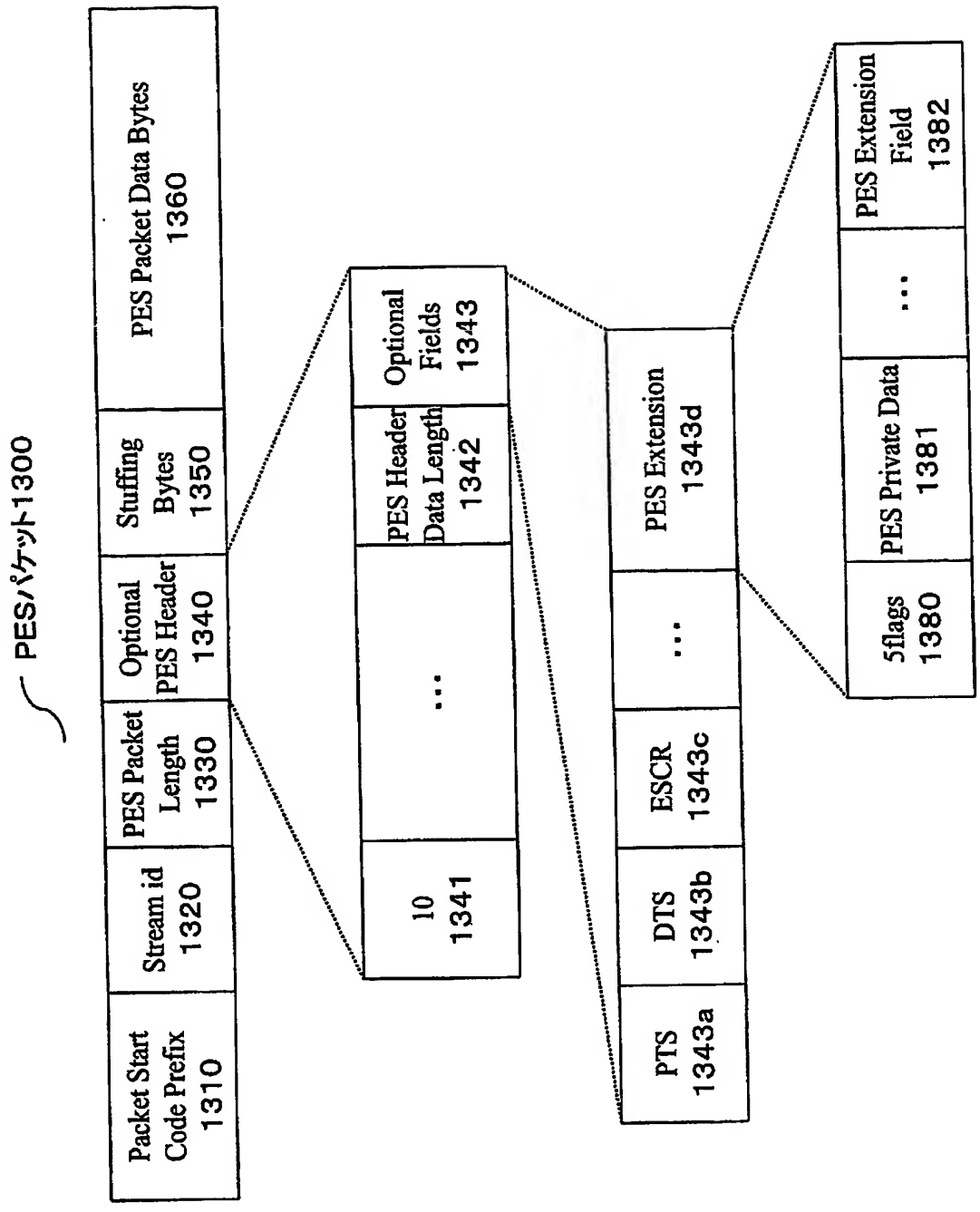
【図１１】


コンテンツ配信サーバ101b
ネットワーク
103
1110
コンテンツ
送出部
1109
コンテンツ
暗号化部
・スクランブル鍵Ks
1108
コンテンツ
多重化部
・ECM-Kw
・ECM-Kc
・Kc配信用ECM
1107
ECM
生成部
・サブライセンス、
・コンテンツ鍵Kc、
・ワーク鍵Kw
権利管理サーバ101a
1104
時刻情報
付加部
・時刻情報
1105
コンテンツ
符号化部
・時刻情報
1106
再生制御情報
生成部
1103
計時部
1101
コンテンツ
DB
1102
コンテンツ
属性情報DB

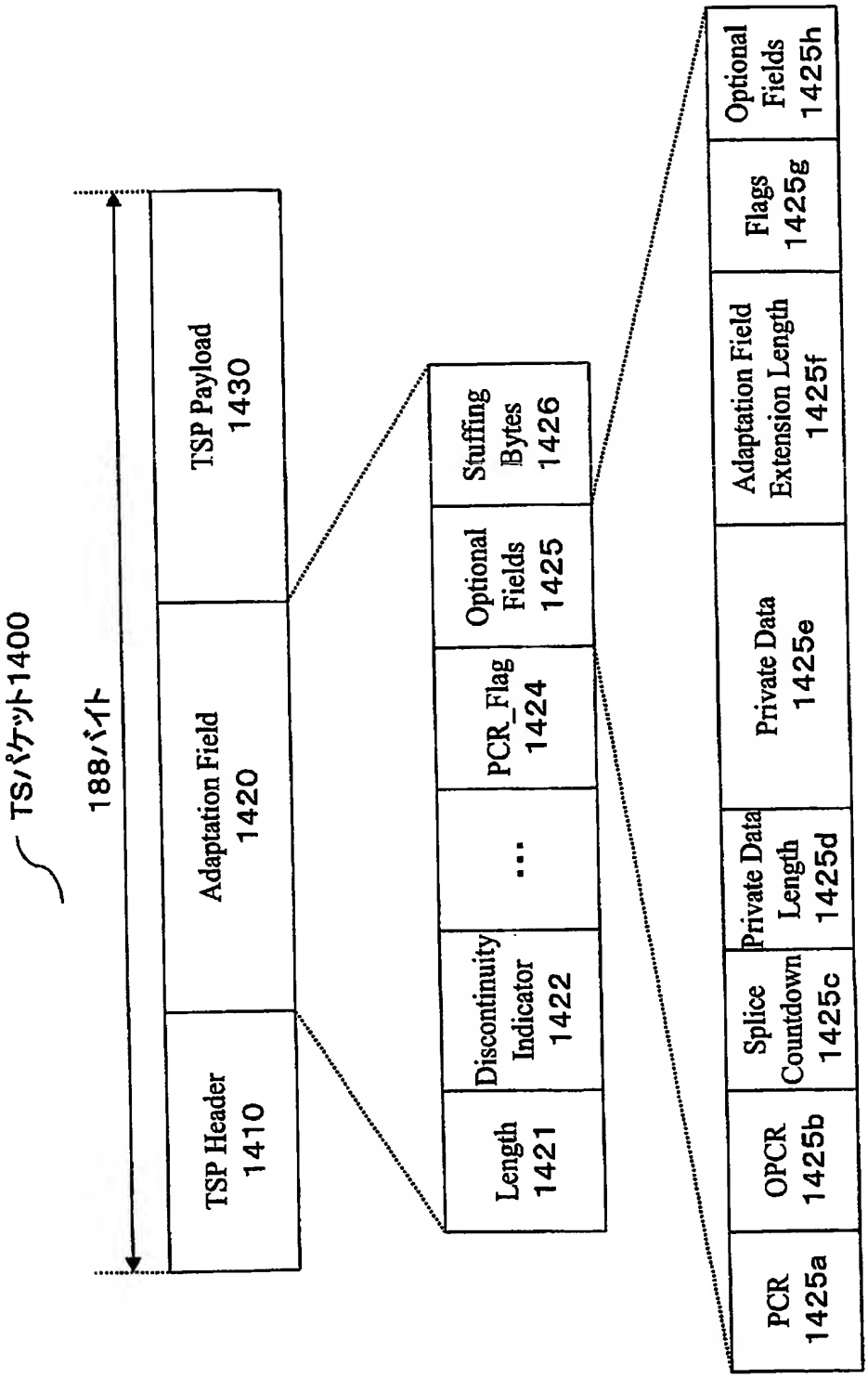
【図１２】


1201
1202
1203
1204
コンテンツID
コンテンツ名称
プレビュー可能区間
CM区間
CONTENT-ID-00001
井上哲也NEWS23
0分～10分
5分～8分
20分～25分
40分～43分
CONTENT-ID-00002
プロダクトX
リアルタイム:
0分～10分
蓄積:
5分～10分:
20分～30分:
コンテンツ属性情報管理テーブル1200

【図１３】


PESパケット1300
Packet Start Code Prefix 1310
Stream id 1320
PES Packet Length 1330
Optional PES Header 1340
Stuffing Bytes 1350
PES Packet Data Bytes 1360
10 1341
...
PES Header Data Length 1342
Optional Fields 1343
PTS 1343a
DTS 1343b
ESCR 1343c
...
PES Extension 1343d
5flags 1380
PES Private Data 1381
...
PES Extension Field 1382

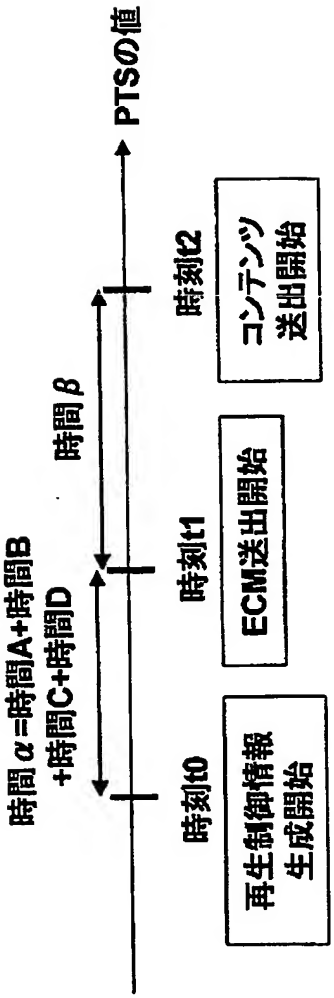
【図１４】


TSパケット1400
188バイト
TSP Header 1410
Adaptation Field 1420
TSP Payload 1430
Length 1421
Discontinuity Indicator 1422
...
PCR_Flag 1424
Optional Fields 1425
Stuffing Bytes 1426
PCR 1425a
OPCR 1425b
Splice Countdown 1425c
Private Data Length 1425d
Private Data 1425e
Adaptation Field Extension Length 1425f
Flags 1425g
Optional Fields 1425h

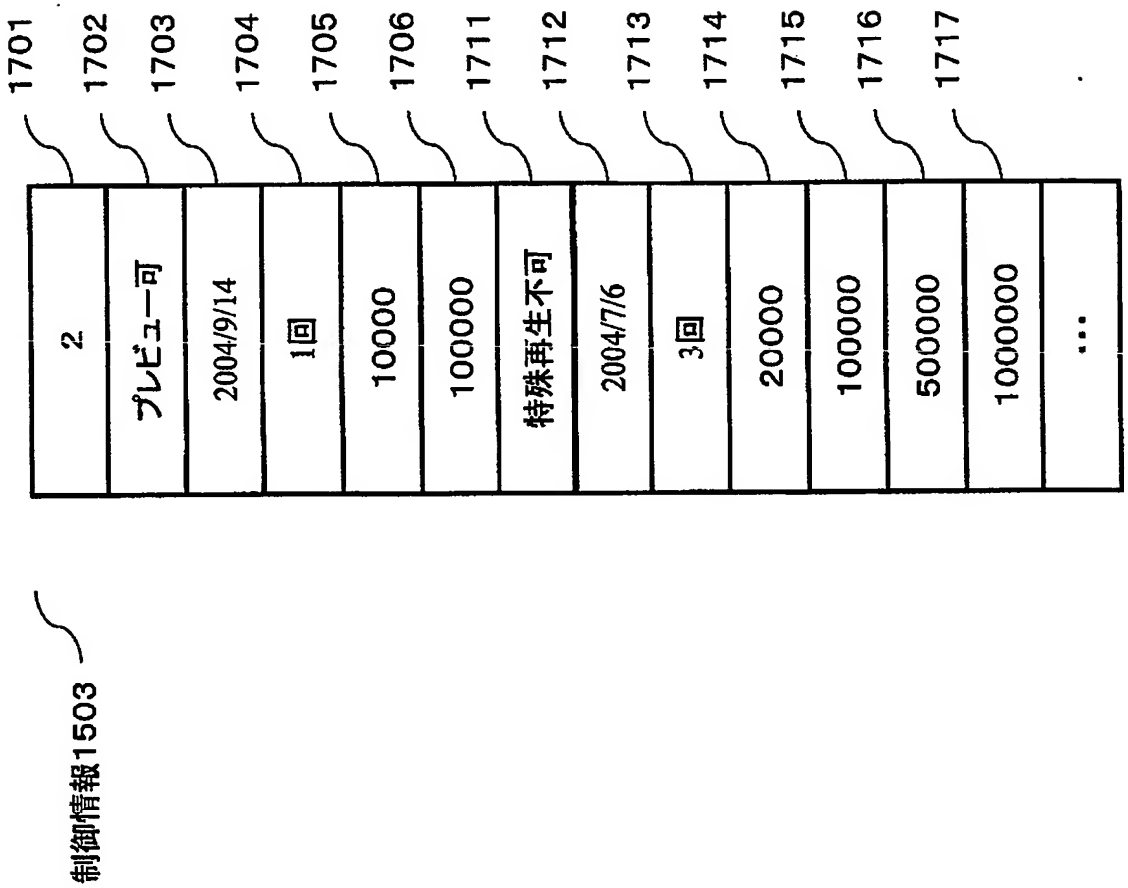
【図１５】

制御情報タグブロック1500
制御情報タグ値
制御情報長
制御情報
1501
1502
1503
制御情報個数
制御ID
制御期限
制御回数
制御範囲
1510
1511
1512
1513
1514
制御時刻個数
制御開始時刻1
制御終了時刻1
...
制御開始時刻n
制御終了時刻n
1520
1521
1522
1523
1524

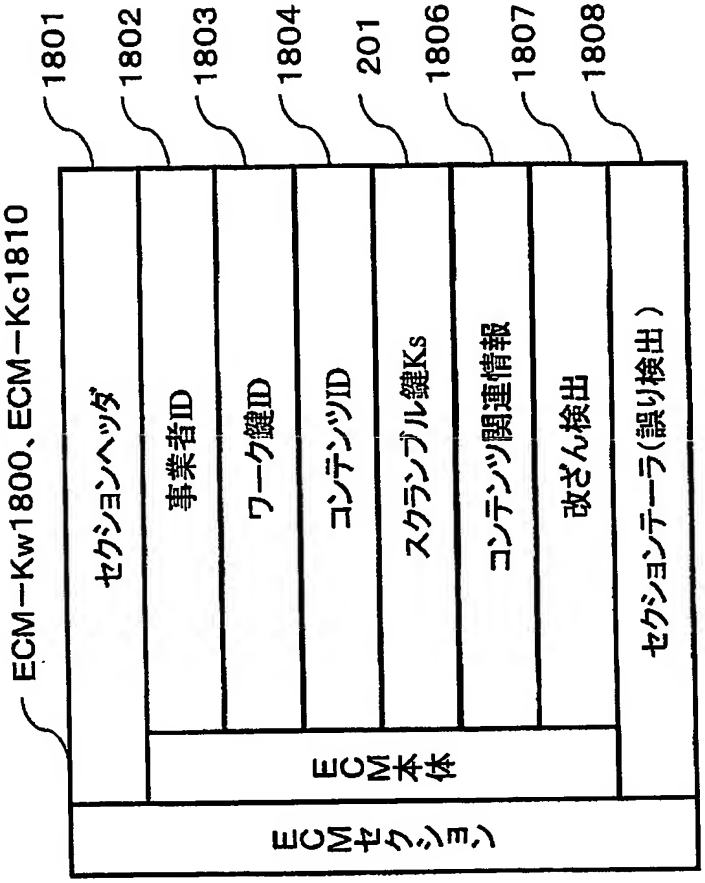
【図１６】


PTSの値
時刻t2
コンテンツ送出開始
時間β
時刻t1
ECM送出開始
時間α=時間A+時間B
+時間C+時間D
時刻t0
再生制御情報生成開始

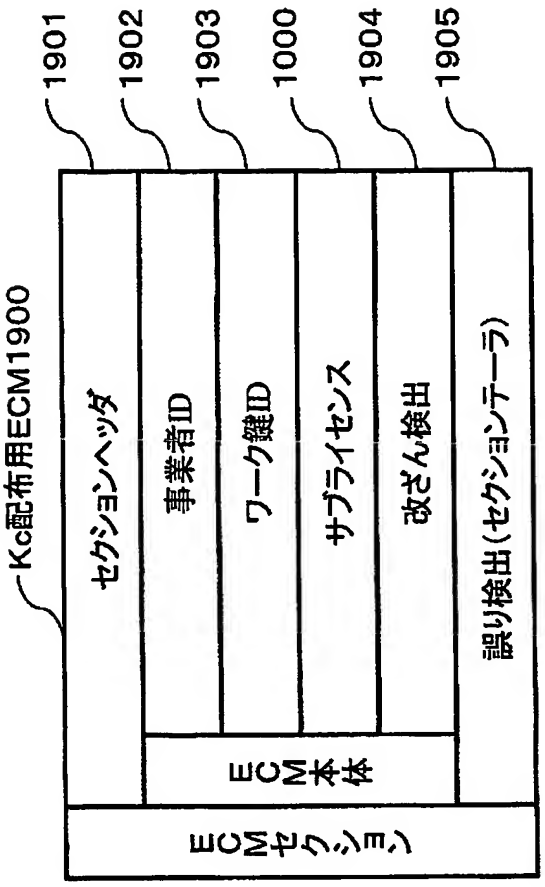
【図１７】


1701
1702
1703
1704
1705
1706
1711
1712
1713
1714
1715
1716
1717
2
プレビュー可
2004/9/14
1回
10000
100000
特殊再生不可
2004/7/6
3回
20000
100000
500000
1000000
...
制御情報1503

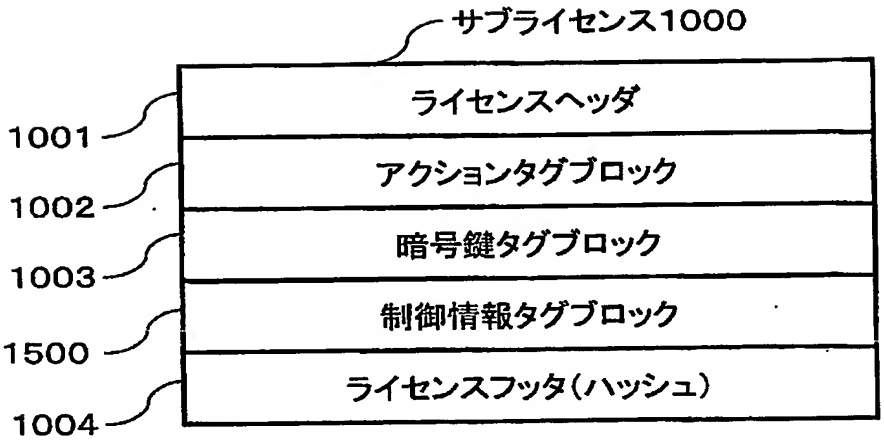
【図１８】


1801
1802
1803
1804
201
1806
1807
1808
ECM−Kw1800、ECM−Kc1810
セクションヘッダ
事業者ID
ワーク鍵ID
コンテンツID
スクランブル鍵Ks
コンテンツ関連情報
改ざん検出
セクションデータ(誤り検出)
ECM本体
ECMセクション

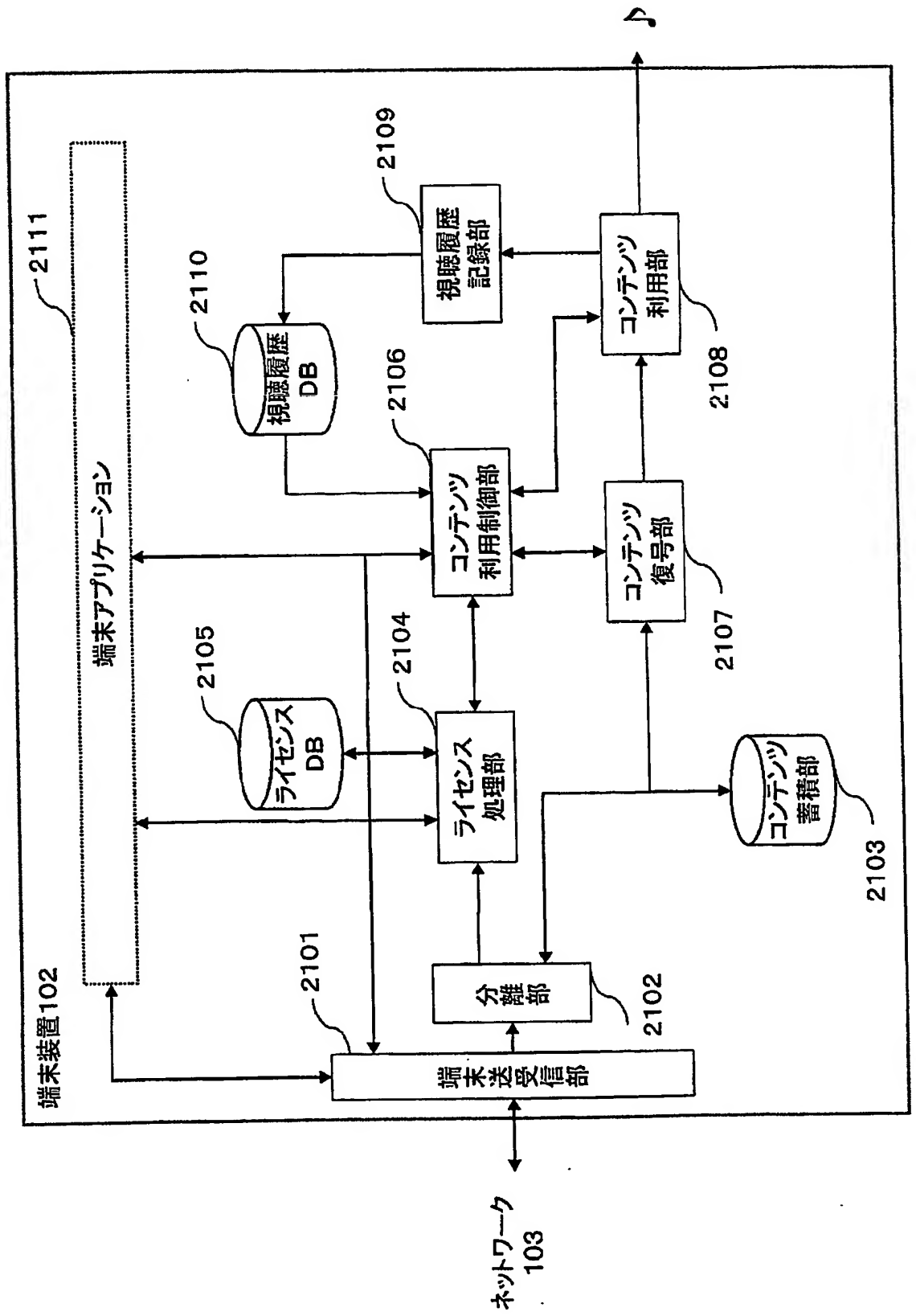
【図１９】


1901
1902
1903
1000
1904
1905
Kc配布用ECM1900
セクションヘッダ
事業者ID
ワーク鍵ID
サプライセンス
改ざん検出
誤り検出（セクションテーラ）
ECM本体
ECMセクション

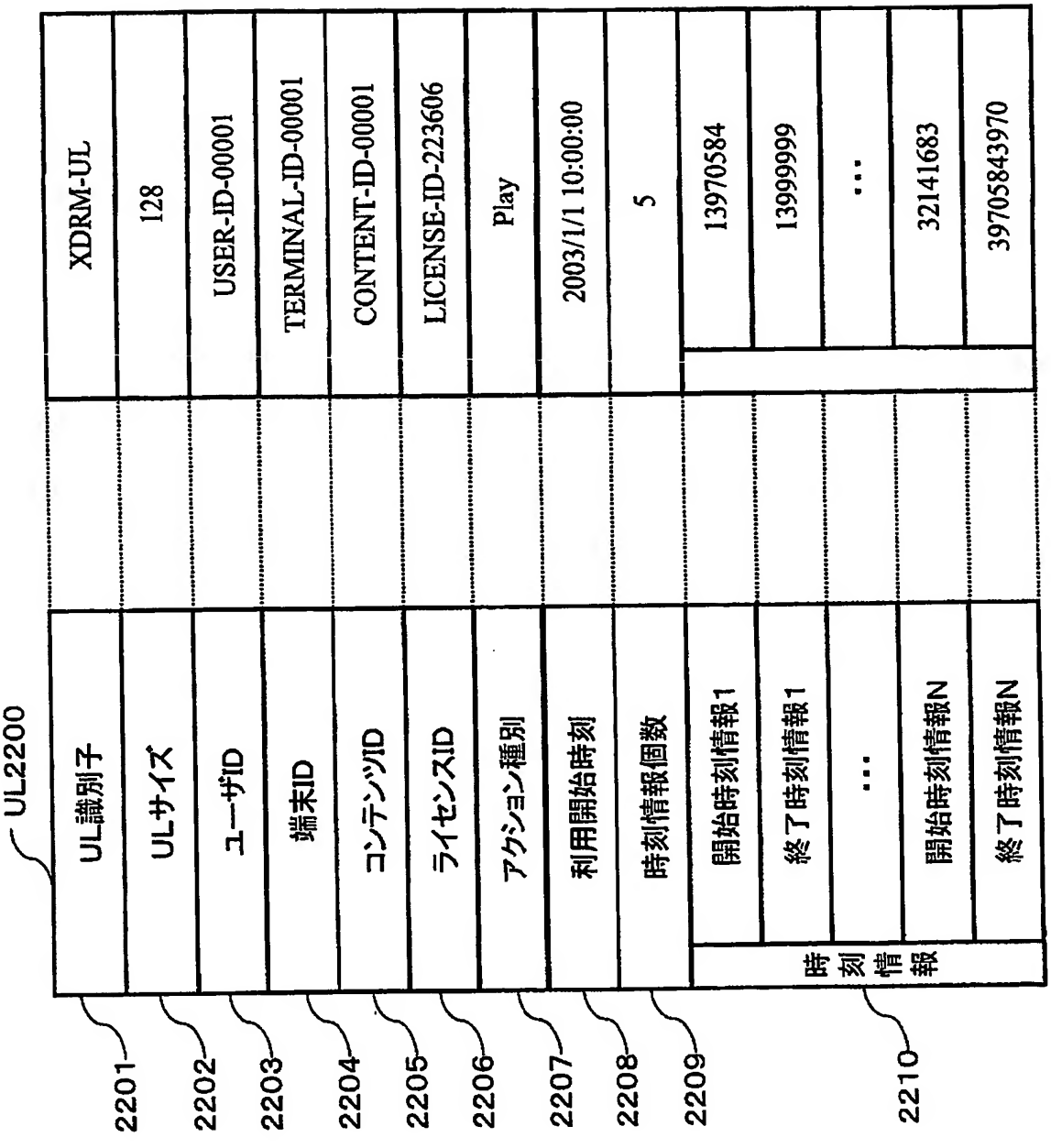
【図２０】


サブライセンス1000
ライセンスヘッダ
1001
アクションタグブロック
1002
暗号鍵タグブロック
1003
制御情報タグブロック
1500
ライセンスフッタ（ハッシュ）
1004

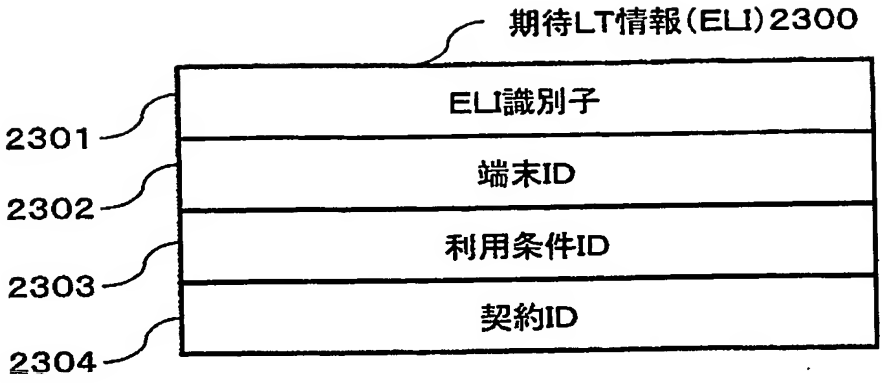
【図２１】


端末装置102
端末アプリケーション
2111
2109
視聴履歴記録部
2110
視聴履歴DB
2106
コンテンツ利用制御部
コンテンツ利用部
2108
コンテンツ復号部
2107
2105
ライセンスDB
2104
ライセンス処理部
コンテンツ蓄積部
2103
2101
分離部
2102
端末送受信部
ネットワーク103

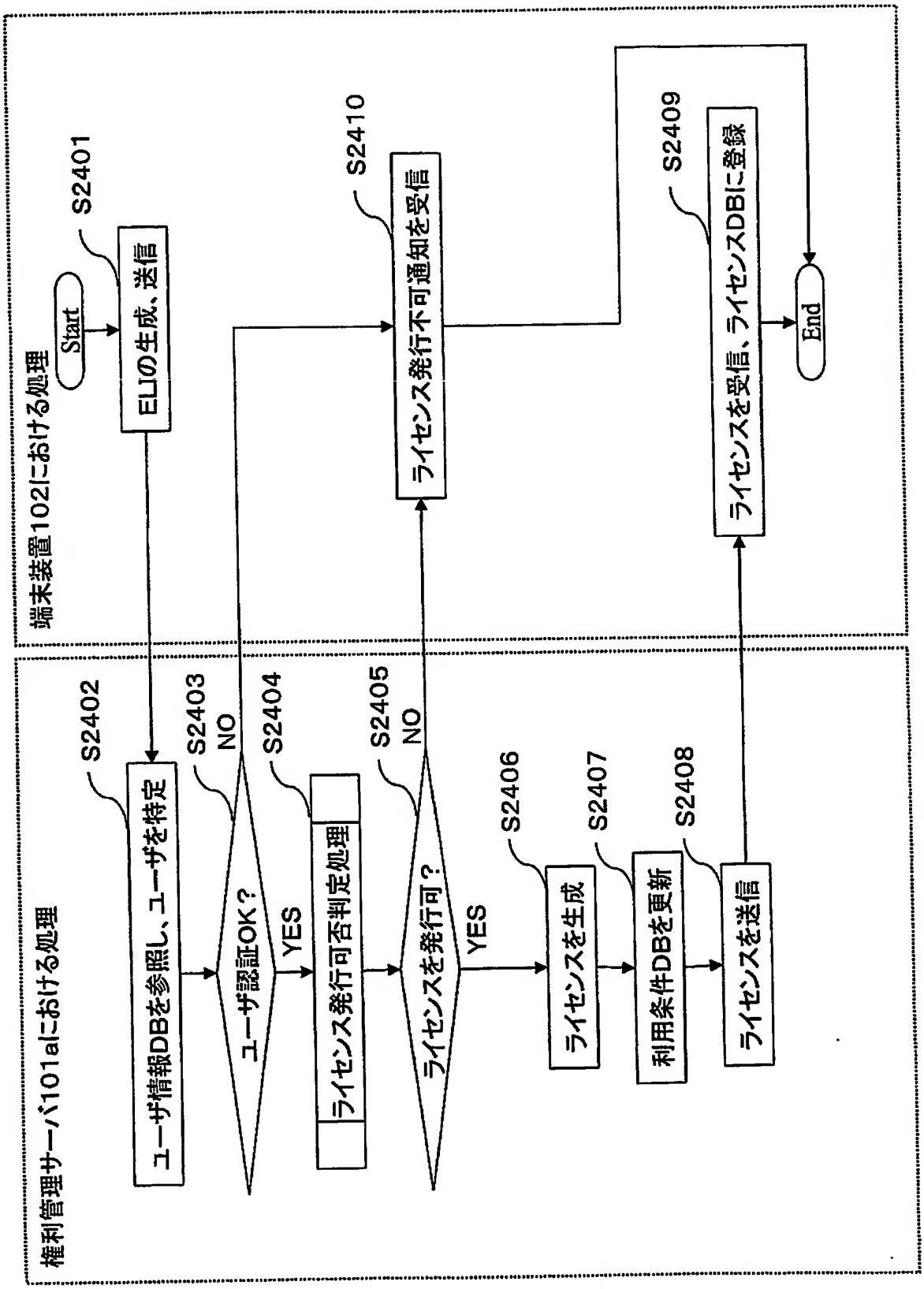
【図２２】


UL2200
UL識別子
XDRM-UL
2201
ULサイズ
128
2202
ユーザID
USER-ID-00001
2203
端末ID
TERMINAL-ID-00001
2204
コンテンツID
CONTENT-ID-00001
2205
ライセンスID
LICENSE-ID-223606
2206
アクション種別
Play
2207
利用開始時刻
2003/1/1 10:00:00
2208
時刻情報個数
5
2209
時刻情報
開始時刻情報1
13970584
終了時刻情報1
13999999
...
...
2210
開始時刻情報N
32141683
終了時刻情報N
39705843970

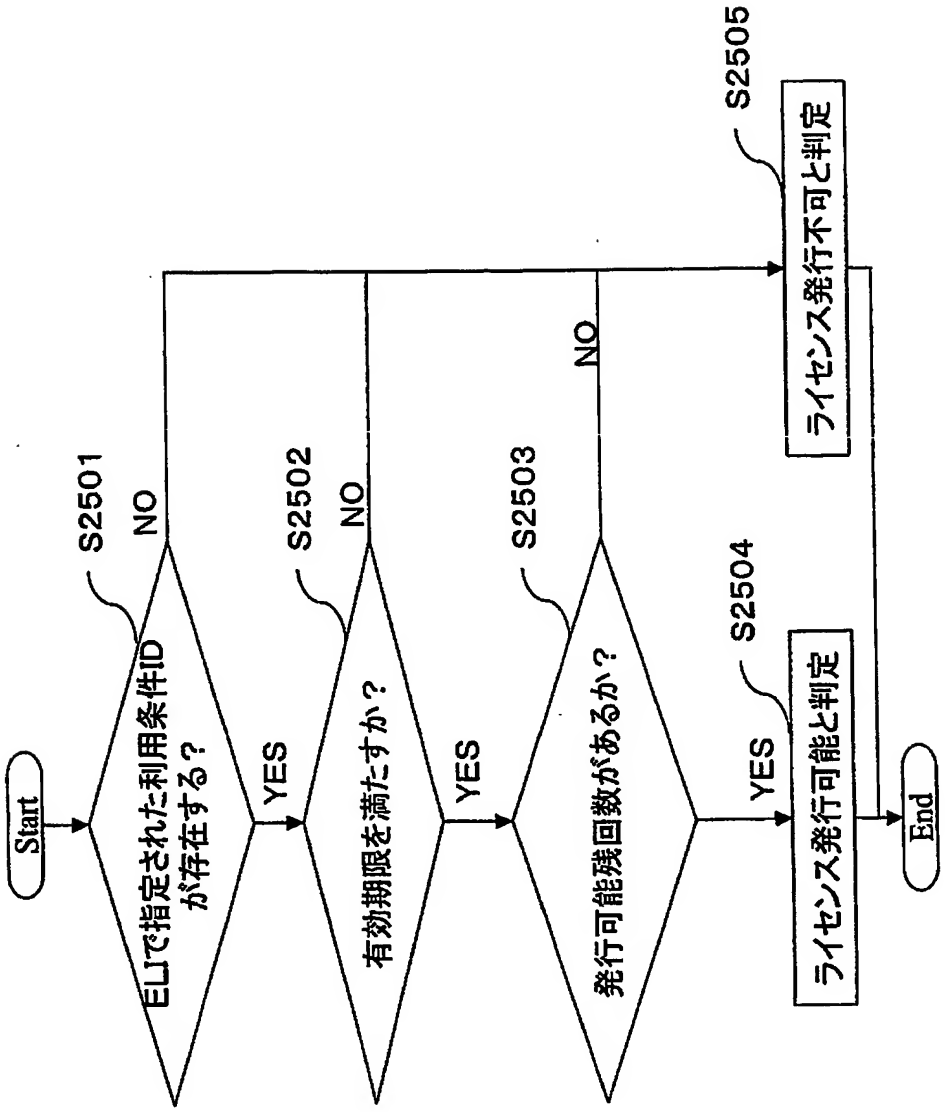
【図２３】



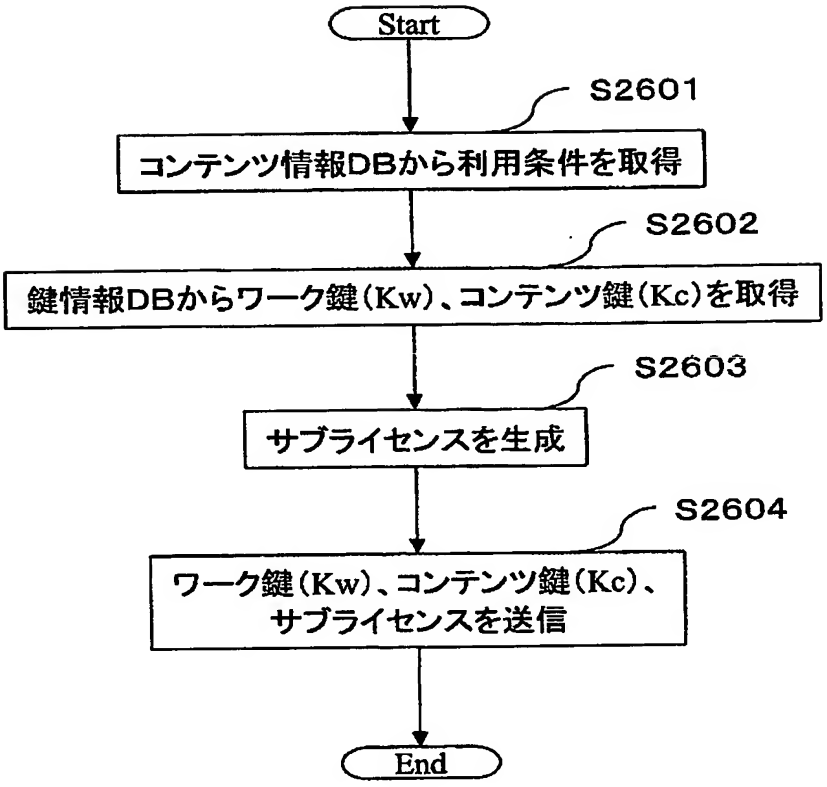
【図２４】


端末装置102における処理
権利管理サーバ101aにおける処理
Start
S2401
ELIの生成、送信
S2402
ユーザ情報DBを参照し、ユーザを特定
S2403
ユーザ認証OK？
NO
YES
S2404
ライセンス発行可否判定処理
S2405
ライセンスを発行可？
NO
YES
S2406
ライセンスを生成
S2407
利用条件DBを更新
S2408
ライセンスを送信
S2410
ライセンス発行不可通知を受信
S2409
ライセンスを受信、ライセンスDBに登録
End

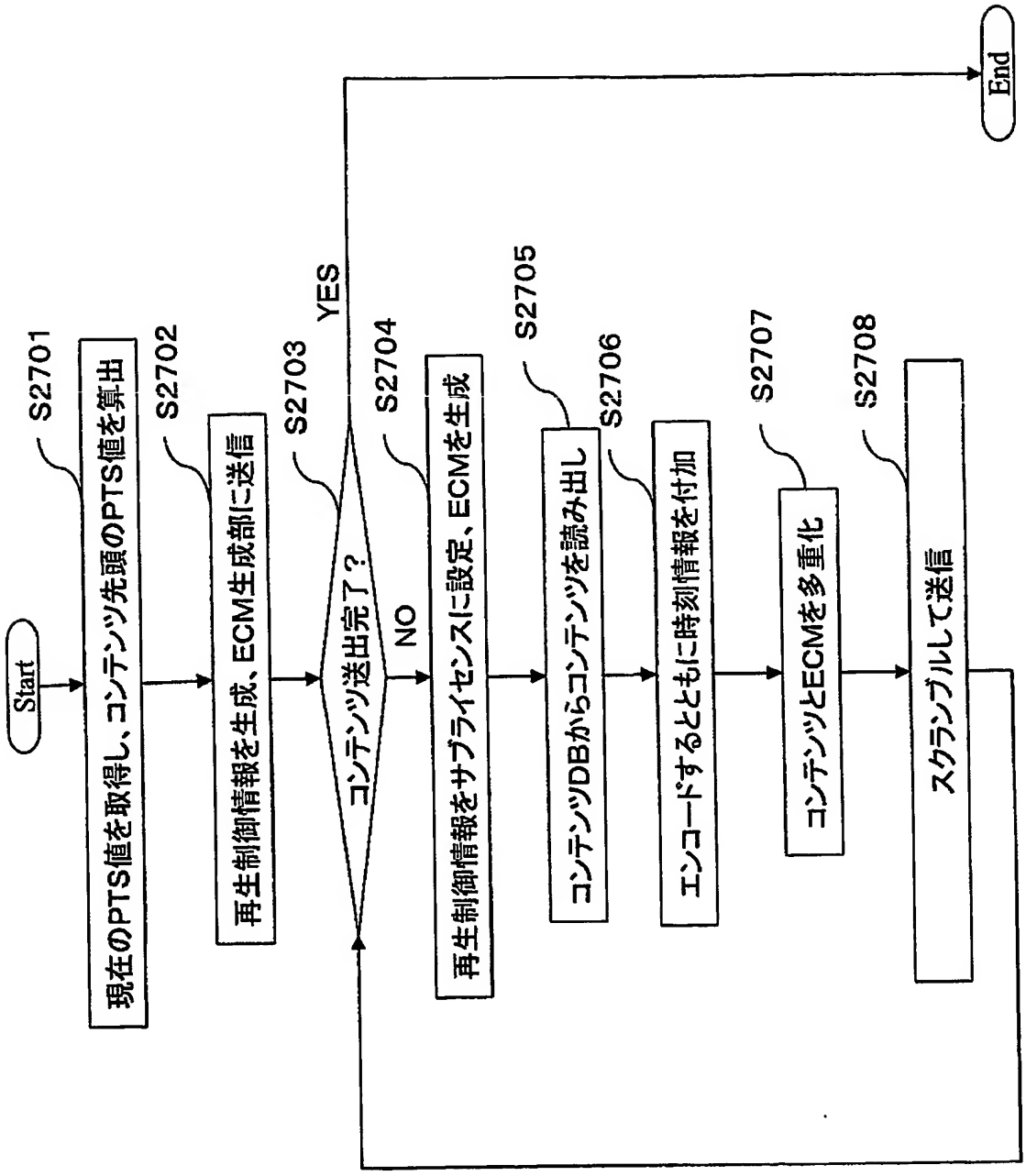
【図２５】


Start
S2501
ELIで指定された利用条件ID
が存在する？
NO
YES
S2502
有効期限を満たすか？
NO
YES
S2503
発行可能残回数があるか？
NO
YES
S2504
ライセンス発行可能と判定
S2505
ライセンス発行不可と判定
End

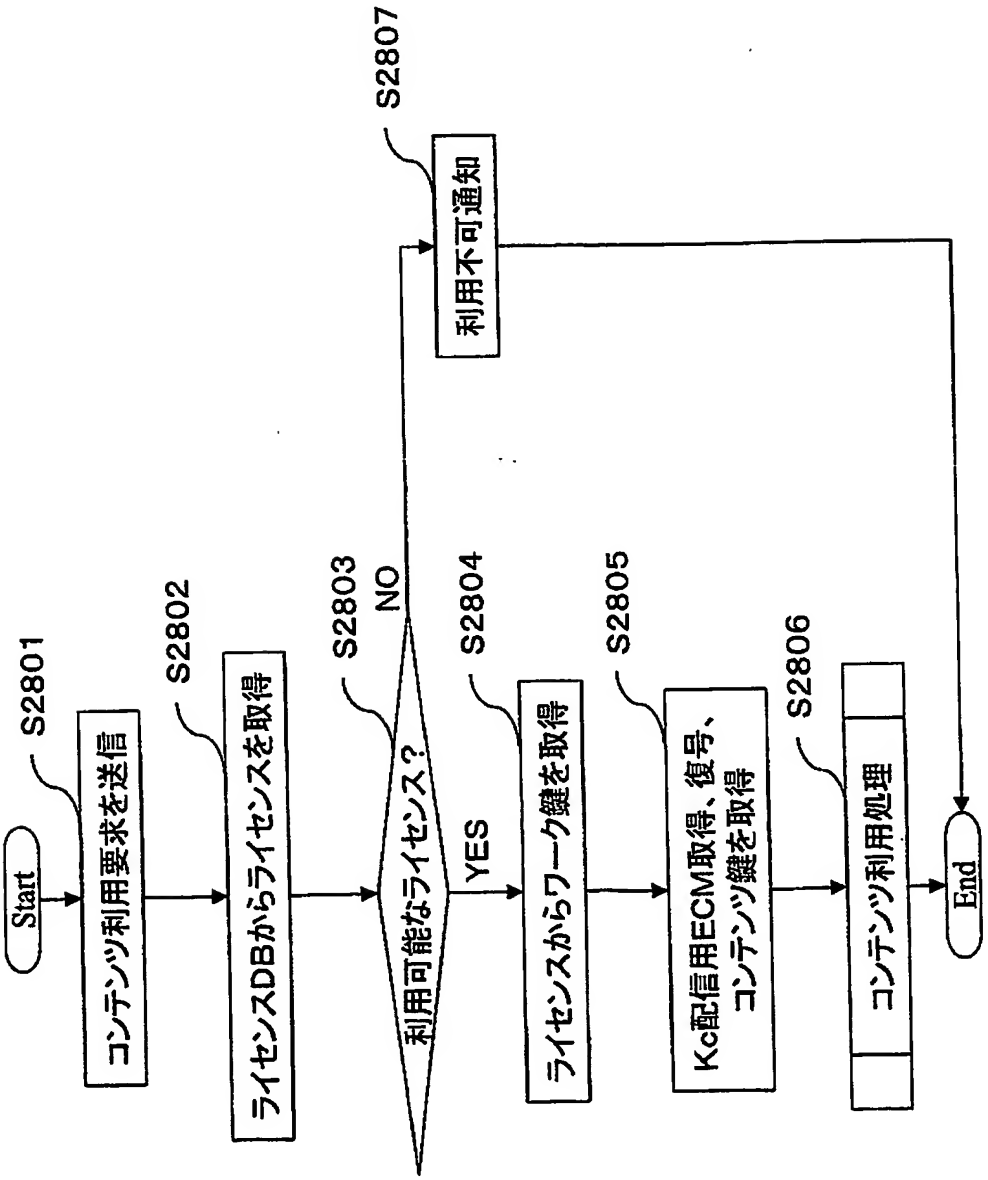
【図２６】


Start
S2601
コンテンツ情報DBから利用条件を取得
S2602
鍵情報DBからワーク鍵(Kw)、コンテンツ鍵(Kc)を取得
S2603
サブライセンスを生成
S2604
ワーク鍵(Kw)、コンテンツ鍵(Kc)、
サブライセンスを送信
End

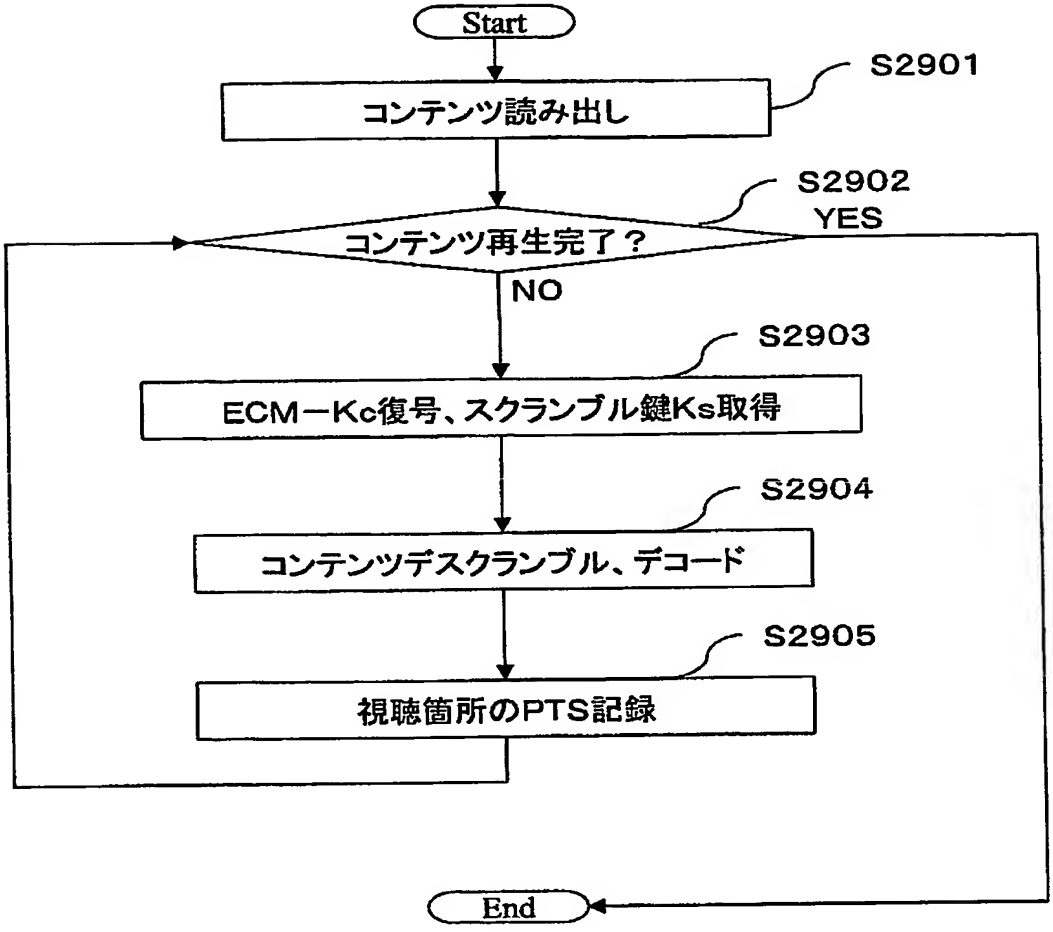
【図２７】


Start
S2701
現在のPTS値を取得し、コンテンツ先頭のPTS値を算出
S2702
再生制御情報を生成、ECM生成部に送信
S2703
コンテンツ送出完了？
YES
End
S2704
NO
再生制御情報をサブライセンスに設定、ECMを生成
S2705
コンテンツDBからコンテンツを読み出し
S2706
エンコードするとともに時刻情報を付加
S2707
コンテンツとECMを多重化
S2708
スクランブルして送信

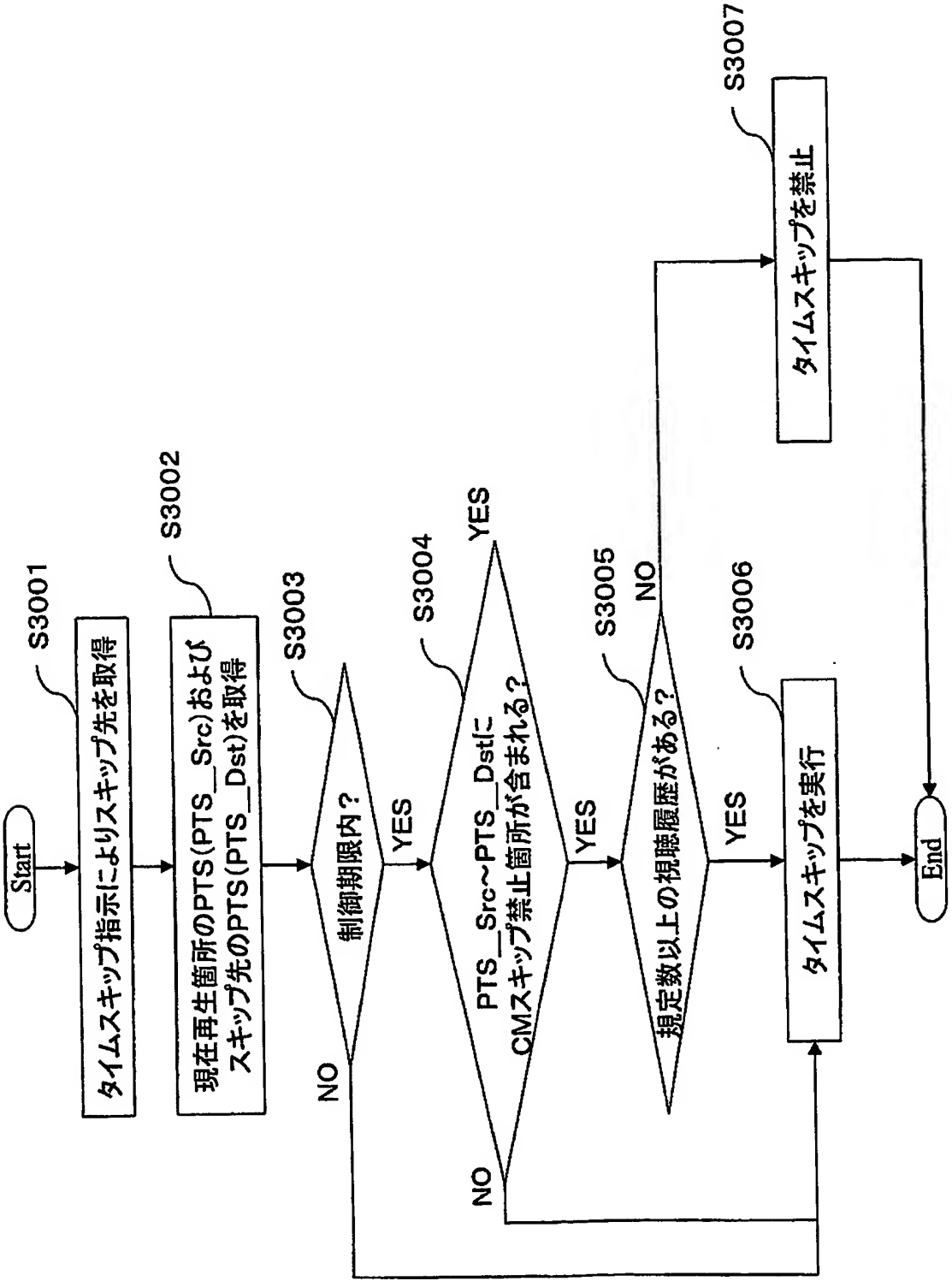
【図２８】


Start
S2801
コンテンツ利用要求を送信
S2802
ライセンスDBからライセンスを取得
S2803
利用可能なライセンス?
NO
YES
S2804
ライセンスからワーク鍵を取得
S2805
Kc配信用ECM取得、復号、コンテンツ鍵を取得
S2806
コンテンツ利用処理
End
S2807
利用不可通知

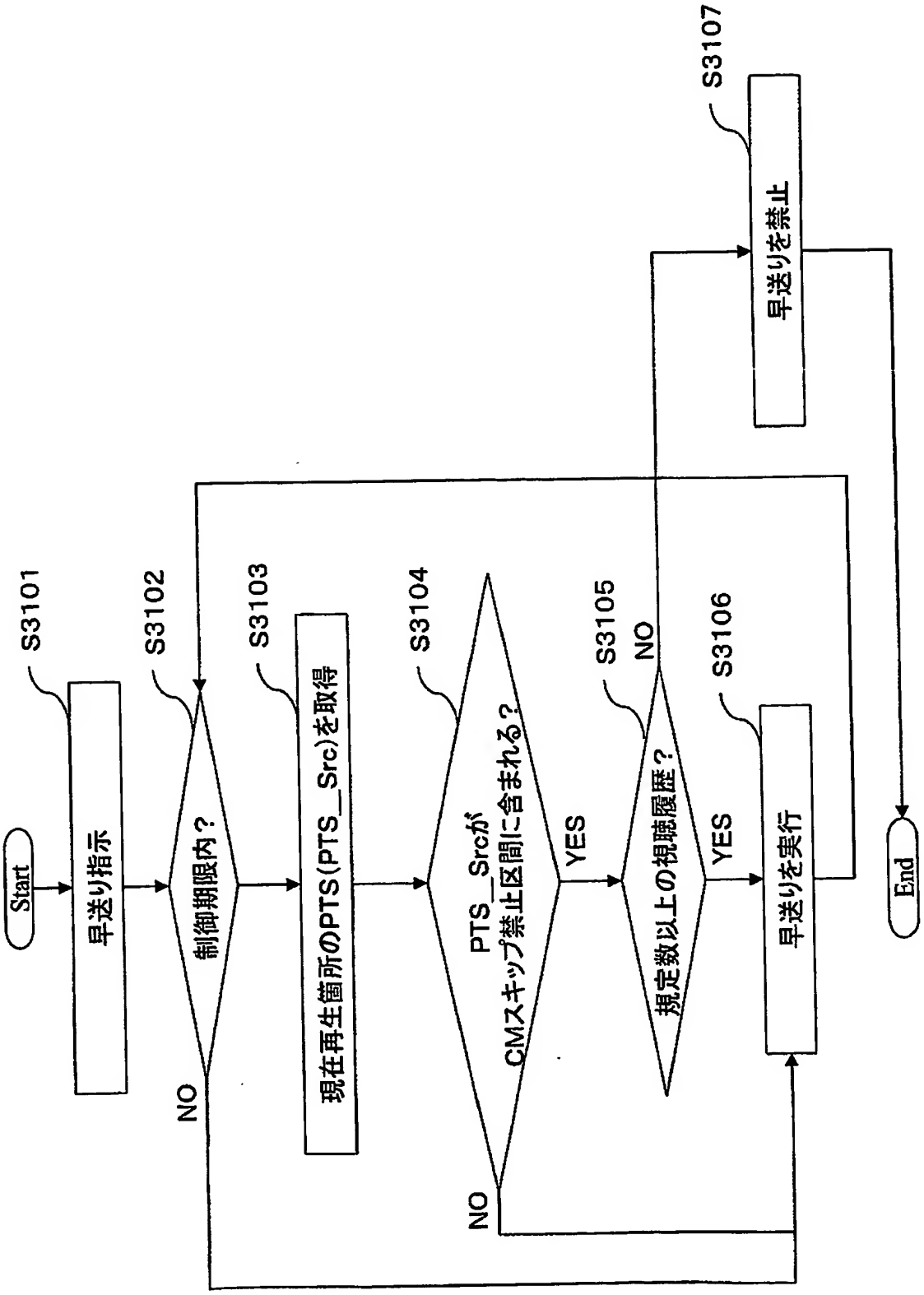
【図２９】


Start
S2901
コンテンツ読み出し
S2902
YES
コンテンツ再生完了？
NO
S2903
ECM－Kc復号、スクランブル鍵Ks取得
S2904
コンテンツデスクランブル、デコード
S2905
視聴箇所のPTS記録
End

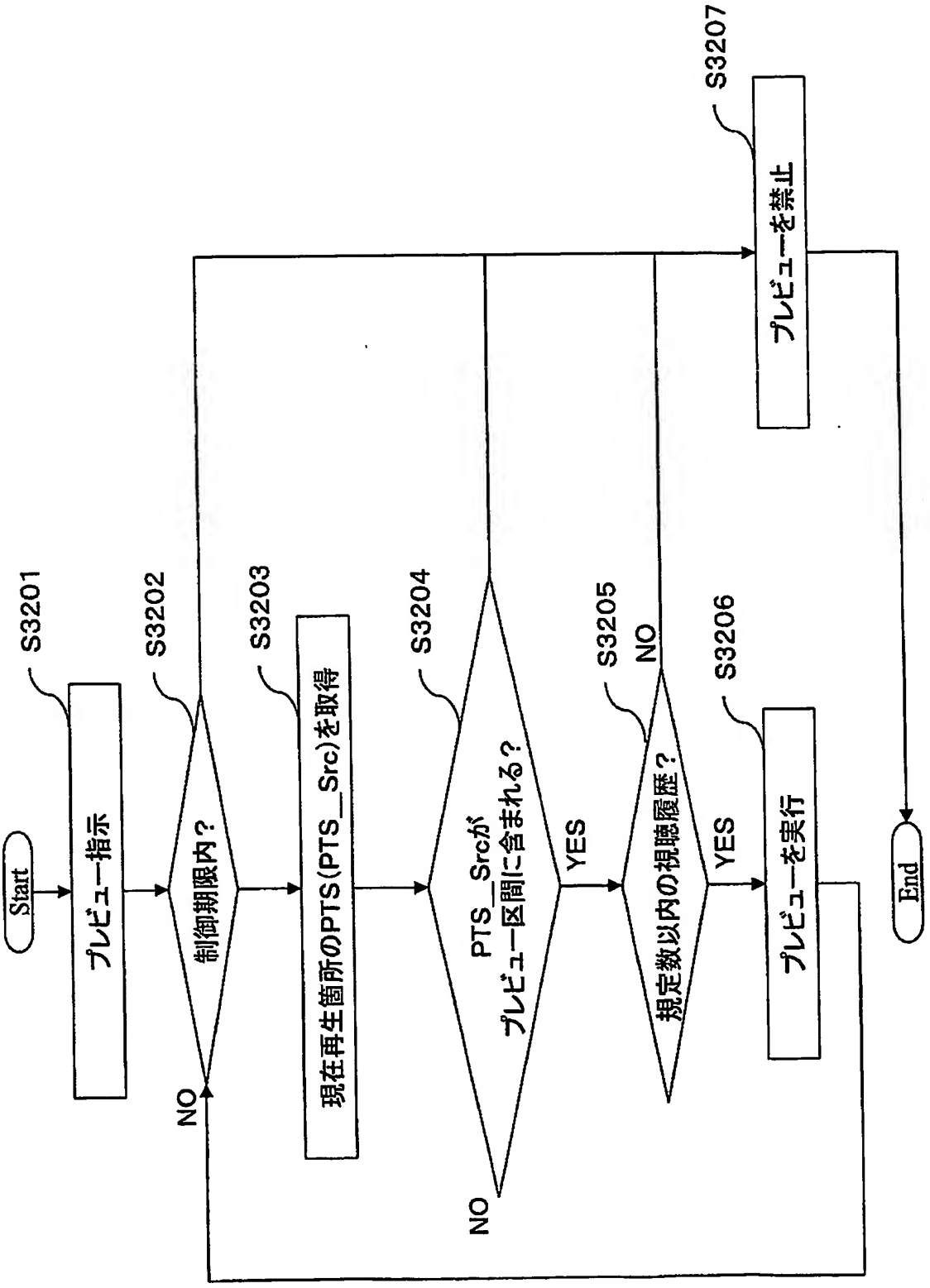
【図３０】


Start
S3001
タイムスキップ指示によりスキップ先を取得
S3002
現在再生箇所のPTS(PTS_Src)およびスキップ先のPTS(PTS_Dst)を取得
S3003
制御期限内？
YES
NO
S3004
PTS_Src～PTS_Dstに
CMスキップ禁止箇所が含まれる？
YES
NO
S3005
規定数以上の視聴履歴がある？
YES
NO
S3006
タイムスキップを実行
S3007
タイムスキップを禁止
End

【図３１】


Start
早送り指示
S3101
制御期限内？
S3102
NO
現在再生箇所のPTS(PTS_Src)を取得
S3103
PTS_Srcが
CMスキップ禁止区間に含まれる？
S3104
YES
NO
規定数以上の視聴履歴？
S3105
YES
早送りを実行
S3106
早送りを禁止
S3107
End

【図３２】


Start
S3201
プレビュー指示
S3202
制御期限内？
NO
S3203
現在再生箇所のPTS(PTS_Src)を取得
S3204
PTS_Srcが
プレビュー区間に含まれる？
NO
YES
S3205
規定数以内の視聴履歴？
NO
YES
S3206
プレビューを実行
S3207
プレビューを禁止
End

【書類名】要約書
【要約】
【課題】　コンテンツに制御情報を追加することなく、事業者が、ユーザのコンテンツ特定部分の利用をセキュアに制御することが可能なコンテンツ利用制御システムを提供する。
【解決手段】　端末装置にコンテンツを配信するコンテンツ配信サーバと、コンテンツの利用をセキュアに制御する端末装置とから構成されるコンテンツ利用制御システムであって、コンテンツ配信サーバは、時刻情報をコンテンツにセキュアに付加するとともに、時刻情報を用いてコンテンツの特定部分の利用を制御するための利用制御情報をコンテンツとは別データとして生成して端末装置に配信し、端末装置は、コンテンツに付加されたセキュアな時刻情報と利用制御情報とを用いて、コンテンツの利用をセキュアに制御する。
【選択図】　図１

認定・付加情報

特許出願の番号	特願２００３－３７８５７４
受付番号	５０３０１８４８２３０
書類名	特許願
担当官	第七担当上席　００９６
作成日	平成１５年１１月１０日

＜認定情報・付加情報＞

【提出日】　平成15年11月 7日

特願２００３－３７８５７４

出願人履歴情報

識別番号　［０００００５８２１］

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社